Norman Access Control Privacy

Benutzerhandbuch

Norman-Publikationsnummer: PRIV-3.0-man-6.4ger-0005

Wichtiger Hinweis zum Copyright

Kein Teil dieser Dokumentation darf in irgendeiner Form (Fotokopie, Aufzeichnungsverfahren oder Systeme zur Informationsspeicherung oder zur Informationsabfrage) ohne die ausdrückliche Genehmigung von Norman zu einem anderen Zweck als dem persönlichen Gebrauch durch den Käufer reproduziert oder unter Verwendung elektronischer Systeme übertragen werden.

Die Informationen in diesem Dokument sowie die Softwarefunktionen können ohne Ankündigung geändert werden. Die Nutzung der Software unterliegt den in der Lizenzvereinbarung festgelegten Bedingungen. Der Käufer ist berechtigt, zu Sicherungszwecken eine Kopie der Software zu erstellen.

Das Norman-Logo ist eine eingetragene Marke von Norman Data Defense Systems.

Die Namen der in dieser Dokumentation erwähnten Produkte, beispielsweise Microsoft®, MS-DOS® oder Windows® sind eingetragene Marken der Microsoft Corporation. Die Namen anderer Produkte sind entweder Marken oder eingetragene Marken ihrer jeweiligen Besitzer. Sie werden nur zu Identifikationszwecken erwähnt.

Für diese Dokumentation und Software gilt
Copyright © Norman Data Defense Systems GmbH, May 16, 2000.
Alle Rechte vorbehalten.

Norman Software License Agreement

ATTENTION:

This license agreement (the "License Agreement") is entered into between you and Norman Data Defense Systems.

This is a license, not a sale. The Norman Data Defense Systems ("Norman", "we" or "us") software product is provided under the following License Agreement which defines what you may do with the Product (as hereinafter defined), and contains limitations on warranties and remedies.

This License Agreement applies to Product(s) for which license is purchased in Norway and outside Norway. In markets where the Product is delivered with a local license agreement, the local license agreement shall be valid and shall prevail in the case of controversy or inconsistency with this License Agreement.

LICENSE

IMPORTANT: You must carefully read this License Agreement before using the Product. If you do not agree to its terms, return the complete Product to the Dealer from which you acquired the license within 15 days of the acquisition, for a full refund. Using the Product indicates that you have read this License Agreement and acknowledged and agreed with its terms.

This License Agreement is your proof of license. Please treat it as valuable property.

1. USE

A. LICENSE: Norman provides you with an electronic version or a storage media containing a computer software program (the "Program"), a user manual and accompanying documents (together called the "Product") and grants you a right to use the Product in accordance with the terms of this License Agreement. The copyright and all other rights with regard to the Product shall remain with us or our suppliers, except for the rights which are expressly granted to you under this License Agreement.

B. YOU MAY:

1. use the Program only according to the specifications in this License Agreement.

Standalone computer use:

You may use the Program on standalone computers. You must acquire a license for one copy of the Program for each computer on which the Program will be installed.

Shared network use:

You may use the Program in a network, provided that you have purchased a number of licenses to the Program which equals the maximum number of copies of the Program in use at any time.

If you wish to use the Program for more users, you will need a further license for each such additional user.

2. make one copy of the Program for archive or back-up purposes.

3. if you have the right to use the Program on your office PC, you may make one copy of the Program for use on your home PC.

Copyright © 2000 Norman

4. transfer the license to use the Program on a permanent basis to a new user provided that you transfer all prior versions and the latest version of the Program. Such a transfer must also include this License Agreement and all documentation accompanying the Program. The new user must agree to the terms of this License Agreement prior to the transfer. We must be notified in writing of such a transfer.

2. RESTRICTIONS

A. YOU MAY NOT:

1. make any changes to the Program, meaning modify, merge, translate, adapt or alter in any manner. Furthermore, you may not perform any type of decompiling, disassembling or reverse engineering to the Program. This does not affect your rights under any legislation implementing the EC Council Directive on the Legal Protection of Computer Programs, including the provisions of the Norwegian Copyright Act Section 39h and Section 39i.

2. loan, license or rent the Program or any copy of it.

3. transfer evaluation versions of the Program for commercial purposes.

3. INTELLECTUAL PROPERTY RIGHTS

Norman Data Defense Systems and its suppliers retain and are the owners of all intellectual property rights to the Product. These rights are protected by intellectual property legislation (including, but not limited to, trademark and copyright laws) in Norway and in foreign jurisdictions and by international treaty provisions.

Norman Data Defense Systems retains all rights to the Product not expressly granted to you.

4. LIMITED WARRANTY

1. We warrant that the Program:

A. substantially conforms with the applicable user documentation. If the Program does not substantially conform with the applicable user documentation, we will, at our option, refund the amount you paid for the Product or issue corrected items at no charge provided that the defective item(s) are returned to us within 90 (ninety) days from the date of purchase.

B. will be distributed on a media that is free from defects with regard to materials and workmanship (this section 4.1.B does not apply if the Program was downloaded in electronic format).

C. will be free from defects with regard to materials and workmanship in the manufacture of the product in a period of 90 days from the date of purchase. We will, at our option, refund the amount you paid for the Product or issue corrected items at no charge provided that the defective item(s) are returned to us within 90 (ninety) days from the date of purchase.

2. If misuse or unauthorised changes occur to the Program, the rights granted to you under this section 4 will not apply.

5. LIMITATION OF LIABLILITY AND WARRANTY

The Product is provided "as is" without any other warranties or conditions, express or implied, including, but not limited to warranties of merchantability, fitness for a particular purpose, or those arising by law, statute, usage of trade or course of dealing - except for the express limited warranty granted to you in section 4 above.

Copyright © 2000 Norman

The entire risk as to the results and performance of the Product is assumed by you. In no event will we be liable for indirect, special, incidental, tort, economic cover or consequential damages arising out of the use of or inability to use the Product, including without limitation, damages or costs relating to the loss of profits, business, goodwill, data or computer programs, even if advised of the possibility of such damages or for claims by a third party. We will in no case be liable for financial damages that exceed the amount paid by you for the license to the Program out of which such a claim arose.

Some states/countries do not allow the exclusion or limitation of implied warranties or limitation of liability for incidental or consequential damages in circumstances which are defined at law. The above limitation may therefore not apply to you.

6. TERM

This License Agreement shall continue for as long as you use the Product. If you have received or downloaded the Product as an evaluation version, this license will only be valid for the period of time the evaluation period lasts. The evaluation period will be stated in the Product and/or in an accompanying offer or on the web site from which it is downloaded.

If you fail to comply with any of its terms or conditions, we have the right to terminate this License Agreement. All copies of the Product must be destroyed if the License Agreement is terminated. The Limitation of Warranties and Liability above shall continue in force even after any termination.

7. GOVERNING LAW

This License Agreement shall be governed and construed in accordance with Norwegian law.

Copyright © 2000 Norman

Beschränkte Garantie

Norman Data Defense Systems garantiert, daß die im Lieferumfang enthaltene CD-ROM und Dokumentation frei von Produktionsfehlern sind. Sollten Sie innerhalb von 30 Tagen nach dem Kauf einen Fehler melden, ersetzt Norman Data Defense Systems die fehlerhafte CD-ROM und/oder Dokumentation kostenlos. Ein Kaufnachweis muß jeder Ersatzforderung beigefügt sein.

Diese Garantie ist auf den Ersatz des Produktes beschränkt. Norman haftet nicht für andere Formen von Verlust oder Schäden, die sich aus der Verwendung der Software oder der Dokumentation oder aus eventuell darin enthaltenen Fehlern oder Mängeln ergeben, einschließlich, aber nicht beschränkt auf, finanzielle Einbußen.

Hinsichtlich Mängeln oder Fehlern der CD-ROM, Diskette oder Dokumentation oder dieser Lizenzvereinbarung hebt diese Garantie alle anderen ausdrücklichen oder stillschweigenden Garantien auf, einschließlich der, jedoch nicht beschränkt auf die, stillschweigenden Garantien für Marktfähigkeit und Eignung für einen bestimmten Zweck.

Insbesondere und ohne die Einschränkungen durch die Lizenzvereinbarung hinsichtlich irgendeiner speziellen Verwendung oder irgendeines speziellen Zwecks haftet Norman in keinem Fall für entgangene Einnahmen oder andere kommerzielle Schäden, einschließlich, jedoch nicht beschränkt auf ursprüngliche und Folgeschäden.

Diese Garantie erlischt 30 Tage nach dem Kauf.

Copyright © 2000 Norman

Norman Data Defense Systems Niederlassungen

Norman Data Defense Systems Pty Ltd
6 Sarton Road, Clayton, Victoria, 3168 **Australien**.
Tel: +61 3 9562 7655 Fax: +61 3 9562 9663
E-mail: norman@norman.com.au
Web: http://www.norman.com.au

Norman Ibas OY
Lakkisepantie 11, 00620 Helsinki, **Finnland**.
Tel: +358 9 477 46 11 Fax: +358 9 477 46120
Web: http://www.norman-ibas.fi

Ibas AS Data Recovery/ Data Erasure
Admin/Sales/Development,
Box 1250 Arkoveien 14, 2206 Kongsvinger, Norwegen.
Tel: +47 62 81 01 00, Fax: +47 62 81 01 50

Norman Data Defense Systems GmbH
Kieler Str. 15, D-42697 Solingen, **Deutschland**.
Tel: +49 212 267 1800 Fax: +49 212 267 1815
E-mail: norman@norman.de Web: http://www.norman.de

Norman/S.H.A.R.K! / ESaSS BV
Postbus 159, NL-2130 AD Hoofddorp, **Niederlande**.
Tel: +31 23 563 3960 Fax: +31 23 561 3165
E-mail: sales@norman.nl Web: http://www.norman.nl

Norman ASA und **Norman Data Defense Systems AB**
Postanschrift: P.O. Box 43, N-1324, Lysaker, **Norwegen**.
Anschrift: Strandveien 37, Lysaker, N-1324 Norway.
Tel: +47 67 10 97 00 Fax: +47 67 58 99 40
E-mail: norman@norman.no Web: http://www.norman.no

Norman Data Defense Systems AG
Postfach CH-4015, Basel, **Schweiz**.
Tel: +41 61 487 2500 Fax: +41 61 487 2501
E-mail: norman@norman.ch Web: http://www.norman.ch

Norman Data Defense Systems (UK) Ltd
Lawn Farm, Oakhill Road, Woodhill, Milton Keyenes, Bucks, MK5 6AH, **Großbritannien**.
Tel: +44 1908 520 900 Fax: +44 1908 520 909
E-mail: norman@normanuk.com Web: http://www.normanuk.com

Copyright © 2000 Norman

Norman Data Defense Systems Inc.
9302 Lee Highway, Suite 950A, Fairfax, VA 22031, **USA**.
Tel: +1703 267 6109 Fax: +1703 934 6368
E-mail: norman@norman.com Web: http://www.norman.com

Schulung und technische Unterstützung

Informationen zu Schulungen oder technischer Unterstützung erhalten Sie bei Ihrem Händler vor Ort oder bei Norman Data Defense Systems.

Copyright © 2000 Norman

Inhalt

Inhalt ix

Zu diesem Handbuch 1

Anwendungsbereich 1
Abkürzungen und Konventionen 1
Weitere Informationen 2
Sagen Sie uns Ihre Meinung 2

Info zu Privacy 3

Wozu Privacy? 3
Systemanforderungen 3
Privacy konfigurieren 3
Was ist Norman Access Control Privacy? 4
Was ist Ver- bzw. Entschlüsselung? 4
Komprimierung der Verschlüsselung 4
Ablaufdaten der Verschlüsselung 4
Schützen Ihrer Daten unabhängig vom Speicherort 5
Daten auf Datenträgern schützen 5
Informationen in Verzeichnissen schützen 6
Informationen in Dateien schützen 6
Text schützen 7
E-Mails schützen 7
Standardmäßige Verschlüsselung und Entschlüsselung 7
Selbstentschlüsselnde Dateien, Verzeichnisse und Datenträger 8
E-Mails verschlüsseln und entschlüsseln 8
E-Mails verschlüsseln 9
E-Mails entschlüsseln 9
Algorithmen 9

Copyright © 2000 Norman

Sicherheitsunterschiede zwischen Algorithmen 10
Private und öffentliche Schlüssel 10
Sonstige Algorithmen 10
Schlüssel und ihre Anordnung 11
Schlüssel 11
Aliasnamen 11
Benutzerprofile 11

Installation 12

Privacy installieren 12

Anmelden bei Privacy 13

Anmelden 13
Vorgehensweise bei der ersten Anmeldung – eine Checkliste 14
Privacy-Dialogfeld jederzeit aufrufen 15
Anmeldekennwort ändern 15

Schlüssel erstellen 17

Dialogfeld Schlüsselverwaltung anzeigen 17
Übersicht über das Dialogfeld Schlüsselverwaltung 17
Schlüssel und Aliasnamen 18
Benutzerprofile 19
Benutzer 21
Benutzer 21
Benutzerkennung hinzufügen 21
Benutzerkennung ändern 23
Benutzerkennung löschen 24
Benutzerprofile 25
Benutzerprofil hinzufügen 25
Benutzerprofilnamen ändern 27
Benutzerprofil exportieren 27
Benutzerprofil importieren 29
Benutzerprofil löschen 30
Aliasnamen und Schlüssel 31

Copyright © 2000 Norman

Aliasnamen und Schlüssel hinzufügen 31
Aliasnamen oder Schlüssel hinzufügen 32
Aliasnamen und Schlüssel löschen 33

Originaldateien 34

Verarbeiten der Originaldateien 34
Dateispezifikationen einstellen 35

Zusätzliche Sicherheitseinstellungen 36

Zusätzliche Sicherheitseinstellungen 36
Zusätzliche Informationen 37
Smartcard-Optionen 37
Voreinstellungen vornehmen 37
Zugriff auf das Dialogfeld „Schlüsselverwaltung“ einschränken 38

Privacy-Algorithmen 39

Algorithmus für Privacy auswählen 39
Anderen Algorithmus einstellen 39

Verschlüsselung 40

Dialogfeld Schlüsselwahl 40
Eine vollständige E-Mail mit oder ohne Anhänge verschlüsseln 41
Text verschlüsseln 43
Datei verschlüsseln – Standard 45
Datei verschlüsseln – selbstentschlüsselnd 47
Verzeichnis verschlüsseln – Standard 48
Datenträger verschlüsseln – Standard 52
Datenträger verschlüsseln – selbstentschlüsselnd 55

Entschlüsseln 57

Dialogfeld Schlüsselwahl 57
Eine vollständige E-Mail mit oder ohne Anhänge entschlüsseln 58
Text entschlüsseln 60

Copyright © 2000 Norman

Datei entschlüsseln – Standard 61

Selbstentschlüsselnde Datei, Verzeichnis oder Datenträger entschlüsseln 63

Inhalt eines verschlüsselten Verzeichnisses anzeigen 64

Einzelne Dateien aus einem verschlüsselten Datenträger oder Verzeichnis entschlüsseln 66

Verschlüsselte Datei im Privacy Viewer entschlüsseln und öffnen 68

Verzeichnis entschlüsseln – Standard 68

Datenträger entschlüsseln – Standard 70

Häufige Fragen 72

Fehlerbehebung 75

Copyright © 2000 Norman

Zu diesem Handbuch

Dieses Handbuch erläutert die Installation, Einrichtung und Anwendung des Norman Access Control Privacy, oder einfach „Privacy“ genannten Datenverschlüsselungspakets von Norman Data Defense Systems.

Bitte lesen Sie das Kapitel ‘Info zu Privacy’ auf Seite 3, um die Konzepte von Privacy kennzulernen. Folgen Sie den Vorgehensweisen im verbleibenden Teil dieses Benutzerhandbuchs, um zu lernen, wie Privacy eingerichtet und verwendet wird.

Anwendungsbereich

Diese Anleitung ist für Systemverwalter und andere Benutzer gedacht, die Norman Privacy installieren, konfigurieren oder verwenden wollen. Der Leser muß mit Windows -Betrieb und -Funktionalität vertraut sein.

Abkürzungen und Konventionen

In diesem Handbuch wird folgende Abkürzung verwendet:

Privacy **Norman Access Control Privacy**

NAC **Norman Access Control for Windows**

Hier sind die in diesem Handbuch verwendeten Konventionen:

Fett kursiv gedruckter Text hebt besonders wichtige Wörter in einem Satz hervor.

➪ Zeigt an, daß für den Abschnitt ein Querverweis auf ein ähnliches Thema vorhanden ist.

Hinweis Ein Hinweis hebt zusätzliche nützliche Informationen hervor, die Sie lesen sollten, um sicherzustellen, daß Sie das Thema oder den Vorgang vollständig verstehen.

Copyright © 2000 Norman

Vorsicht

Unter dem Titel „Vorsicht“ finden Sie sehr wichtige Informationen, die Sie unbedingt lesen müssen. Wenn Sie diese Informationen nicht lesen, können Sie auf schwerwiegende Sicherheitsprobleme stoßen.

WARNUNG

Eine Warnung enthält Informationen, die Sie UNBEDINGT LESEN MÜSSEN. Wenn Sie die Warnung nicht lesen, können Sie unter Umständen ALLE Daten auf Ihrer Workstation verlieren.

Weitere Informationen

Wenn Sie die gewünschten Informationen in diesem Handbuch nicht finden können, klicken Sie in jedem beliebigen Privacy-Dialogfeld auf die Schaltfläche „Hilfe“. Privacy enthält auch eine Online-Hilfe.

Sagen Sie uns Ihre Meinung

Wir von Norman Data Defense Systems sind bemüht, Ihnen möglichst informative, exakte und nützliche Handbücher zur Verfügung zu stellen.

Wenn Sie Anmerkungen zu diesem oder einem anderen Handbuch von Norman Data Defense Systems haben, senden Sie bitte eine E-Mail an folgende Adresse:

norman@norman.com.au

oder wenden Sie sich an das nächste Norman Data Defense Systems-Büro, Einzelheiten finden Sie auf page vii.

Wir sind für jede Reaktion sehr dankbar.

Copyright © 2000 Norman

Info zu Privacy

Wozu Privacy?

Datenschutz kann aus vielerlei Gründen erforderlich werden. Wenn Sie Internet- oder E-Mail-Funktionen verwenden, kann Ihre Privatkorrespondenz von jedem eingesehen werden, der weiß, wie sie zu lesen ist. Das mag bei gewöhnlichen Nachrichten durchaus akzeptabel sein – jedoch nicht, wenn sie speziellen Text oder Dateien enthalten, die nur für den Empfänger lesbar sein sollen.

Vielleicht besitzen Sie einen portablen Notebook-Computer mit vertraulichen Daten. Was wäre, wenn die Festplatte in falsche Hände geriete? Welche Auswirkungen hätte es für Ihre Firma, wenn Ihre Mitbewerber die Daten „entdeckte“?

Aus welchen Gründen Sie auch immer Ihre Daten schützen möchten, Sie brauchen Privacy.

Systemanforderungen

Sie können Privacy auf jedem Computer mit einem Intel-kompatiblen Prozessor installieren, auf dem Windows® 95, Windows® 98 oder Windows NT® Version 4.X ausgeführt wird.

Privacy konfigurieren

Bevor Sie Privacy konfigurieren, sollten Sie dieses Kapitel lesen, um die Grundlagen von Privacy, Verschlüsselung, Entschlüsselung und Algorithmen kennenzulernen, und um zu erfahren, welche Informationen Privacy schützen kann.

➪ Nachdem Sie Privacy installiert und sich angemeldet haben, fahren Sie mit dem Abschnitt ‘Vorgehensweise bei der ersten Anmeldung – eine Checkliste’ auf Seite 14 fort.
Die Standard-Benutzerkennung und das Kennwort zum Anmelden lauten *Admin* und *admin*.

Copyright © 2000 Norman

Was ist Norman Access Control Privacy?

Privacy ist eine Anwendung zur Verschlüsselung und Entschlüsselung. Verwenden Sie Privacy zum Verschlüsseln und Entschlüsseln folgender Elemente:

- E-Mails und E-Mail-Anhänge,
- jedes Texts, der ausgeschnitten und eingefügt werden kann (z. B. ein Abschnitt aus einer E-Mail oder der Inhalt einer Zelle in einer Tabellenkalkulation),
- einer Datei,
- eines Verzeichnisses oder
- aller Benutzerdaten auf einem Wechseldatenträger.

Was ist Ver- bzw. Entschlüsselung?

Durch Verschlüsselung werden Daten für jeden unkenntlich gemacht, der über keinen Schlüssel zu ihrer Entzifferung verfügt. Aus „Hallo“ kann beispielsweise „2kdi&k4“ werden.

Nach der Verschlüsselung können die Daten nur von Ihnen und von Ihnen ausgewählten Personen wieder lesbar gemacht werden.

Komprimierung der Verschlüsselung

Wenn Sie Daten verschlüsseln, können Sie Privacy so einstellen, daß die Informationen vor dem Verschlüsseln automatisch komprimiert werden.

Wenn Sie beispielsweise Text in einem Dokument verschlüsseln, der 10 Seiten umfaßt, wird durch die Komprimierung die Anzahl der benötigten verschlüsselten Seiten auf fünf Seiten reduziert. Beim Verschlüsseln von anderen Informationen (eine Datei, ein Verzeichnis oder ein Wechseldatenträger), wird durch eine Komprimierung der zum Speichern der verschlüsselten Informationen erforderliche Speicherplatz reduziert.

Ablaufdaten der Verschlüsselung

Wenn Sie Informationen verschlüsseln, können Sie ein Ablaufdatum für die Verschlüsselung festlegen. Ab diesem Datum kann auf die verschlüsselten Daten nicht mehr zugegriffen werden (niemand kann sie mehr entschlüsseln).

Copyright © 2000 Norman

Nehmen wir an, Sie speichern einige verschlüsselte Informationen auf einem Computer, zu dem ein unbefugter Benutzer Zugang hat, beispielsweise ein Notebook-Computer, den Sie jeden Tag vom Büro mit nach Hause nehmen. Wenn Sie für die verschlüsselten Informationen ein Ablaufdatum festlegen, das nur wenige Tage entfernt ist, hat ein Unbefugter wenig Zeit, die verschlüsselten Informationen zu entschlüsseln.

Schützen Ihrer Daten unabhängig vom Speicherort

Daten auf Datenträgern schützen

Über den Windows Explorer können Sie alle Daten auf einem *Wechseldatenträger* ver- und entschlüsseln. Dabei haben Sie die Möglichkeit, den gesamten Text, alle Bilder und Grafiken, entweder nur des Hauptverzeichnisses oder des gesamten Wechseldatenträgers, zu verschlüsseln.

Sie können zwei Arten von verschlüsselten Datenträgern erstellen:

- einen standardmäßig verschlüsselten Datenträger und
- einen selbstentschlüsselnden Datenträger.

Beim Entschlüsseln des Datenträgers können Sie folgendes tun

- den gesamten Inhalt des Datenträgers auf einmal entschlüsseln,
- den Inhalt des Datenträgers im *Privacy Viewer* anzeigen und nur bestimmte Dateien entschlüsseln oder
- den Inhalt des Datenträgers im *Privacy Viewer* anzeigen und auf eine Datei doppelklicken, um sie zu entschlüsseln und zu öffnen.

Hinweis Privacy verschlüsselt nicht die Systembereiche eines Wechseldatenträgers. Wenn Sie einen gesamten Datenträger oder Ihre Festplatte verschlüsseln möchten, verwenden Sie die Festplattenverschlüsselung von Norman Access Control (NAC) für Windows 95/98, NAC für Windows NT oder NAC für Notebooks.

➪ ‘Datenträger verschlüsseln – Standard’ auf Seite 52, ‘Datenträger verschlüsseln – selbstentschlüsselnd’ auf Seite 55, ‘Einzelne Dateien aus einem verschlüsselten Datenträger oder Verzeichnis entschlüsseln’ auf Seite 66 und ‘Verschlüsselte Datei im Privacy Viewer entschlüsseln und öffnen’ auf Seite 68.

Copyright © 2000 Norman

Informationen in Verzeichnissen schützen

Sie können Verzeichnisse in Windows Explorer oder in einem seiner folgenden Dialogfelder verschlüsseln: Speichern, Speichern unter, Öffnen und Suchen. Sie können den gesamten Text, alle Bilder oder Grafiken eines Verzeichnisses oder eines Verzeichnisses mit allen Unterverzeichnissen verschlüssen (rekursive Verschlüsselung).

Sie können zwei Arten von verschlüsselten Verzeichnissen erstellen:

- ein standardmäßig verschlüsseltes Verzeichnis und
- ein selbstentschlüsselndes Verzeichnis.

Beim Entschlüsseln des Verzeichnisses können Sie folgendes tun

- den gesamten Inhalt des Verzeichnisses auf einmal entschlüsseln,
- den Inhalt des Verzeichnisses im *Privacy Viewer* anzeigen und nur bestimmte Dateien entschlüsseln oder
- den Inhalt des Verzeichnisses im *Privacy Viewer* anzeigen und auf eine Datei doppelklicken, um sie zu entschlüsseln und zu öffnen.

➪ ‘Verzeichnis verschlüsseln – Standard’ auf Seite 48, ‘Datei verschlüsseln – selbstentschlüsselnd’ auf Seite 47, ‘Einzelne Dateien aus einem verschlüsselten Datenträger oder Verzeichnis entschlüsseln’ auf Seite 66 und ‘Verschlüsselte Datei im Privacy Viewer entschlüsseln und öffnen’ auf Seite 68.

Informationen in Dateien schützen

Sie können jede Datei in Windows Explorer oder in einem seiner folgenden Dialogfelder verschlüsseln: Speichern, Speichern unter, Öffnen und Suchen. Dabei wird der gesamte Dateiinhalt verschlüsselt, einschließlich Text, Bildern und Grafiken.

Sie können zwei Arten von verschlüsselten Dateien erstellen:

- eine standardmäßig verschlüsselte Datei und
- eine selbstentschlüsselnde Datei.

➪ ‘Standardmäßige Verschlüsselung und Entschlüsselung’ auf Seite 7, ‘Selbstentschlüsselnde Dateien, Verzeichnisse und Datenträger’ auf Seite 8, ‘Datei verschlüsseln – Standard’ auf Seite 45 und ‘Datei verschlüsseln – selbstentschlüsselnd’ auf Seite 47.

Copyright © 2000 Norman

Text schützen

Text kann aus einer beliebigen die Zwischenablage unterstützenden Anwendung heraus ver- und entschlüsselt werden. Zur Verschlüsselung kopieren Sie den Text in die Zwischenablage und verschlüsseln ihn, bevor sie ihn wieder in die Anwendung zurückkopieren. Zum Lesen kopieren Sie den Text in die Zwischenablage und entschlüsseln ihn mit dem richtigen Schlüssel.

Beim Verschlüsseln von Text geht die gesamte Textformatierung verloren.

➪ ‘Text verschlüsseln’ auf Seite 43.

E-Mails schützen

Sie können E-Mail-Nachrichten mit oder ohne Anhänge ver- und entschlüsseln. Dabei wird der gesamte Inhalt eines Anhangs verschlüsselt, einschließlich Text, Bildern und Grafiken. Sie können auch selbstentschlüsselnde Anhänge erstellen.

Standardmäßige Verschlüsselung und Entschlüsselung

Wenn Sie eine Standardverschlüsselung durchführen, verschlüsselt Privacy den gesamten Inhalt eines Datenträgers, Verzeichnisses oder einer Datei und legt das Ergebnis in einer einzelnen *.Encrypted*-Datei ab. Sie können die Informationen komprimieren, bevor sie von Privacy verschlüsselt werden.

Zum Entschlüsseln der *.Encrypted*-Datei können Sie folgendes tun

- die gesamte *.Encrypted*-Datei auf einmal entschlüsseln,
- den Inhalt der *.Encrypted*-Datei im *Privacy Viewer* anzeigen und eine oder mehrere Dateien zur Entschlüsselung auswählen. (Nur bei verschlüsselten Datenträgern und Verzeichnissen.)
- die *.Encrypted*-Datei im *Privacy Viewer* anzeigen und auf eine Datei doppelklicken, um sie zu entschlüsseln und zu öffnen. (Nur bei verschlüsselten Datenträgern und Verzeichnissen.)

Copyright © 2000 Norman

Selbstentschlüsselnde Dateien, Verzeichnisse und Datenträger

Eine selbstentschlüsselnde Datei, ein selbstentschlüsselndes Verzeichnis oder einen selbstentschlüsselnden Datenträger können Sie ohne spezielle Software entschlüsseln.

Wenn Sie eine selbstentschlüsselnde Datei, ein selbstentschlüsselndes Verzeichnis oder einen selbstentschlüsselnden Datenträger erstellen, komprimiert Privacy die Informationen und verschlüsselt sie dann, um eine Datei *.Encrypted.exe* zu erstellen.

Sie können die Datei *.Encrypted.exe* auf einem beliebigen Computer entschlüsseln – Privacy muß dazu nicht installiert sein. Sie müssen nur auf die Datei *.Encrypted.exe* doppelklicken und den Schlüssel eingeben. So einfach ist das!

➪ ‘Datei verschlüsseln – selbstentschlüsselnd’ auf Seite 47, ‘Verzeichnis verschlüsseln – selbstentschlüsselnd’ auf Seite 51 und ‘Datenträger verschlüsseln – selbstentschlüsselnd’ auf Seite 55.

E-Mails verschlüsseln und entschlüsseln

Wenn Sie eine E-Mail versenden, möchten Sie sicherlich ausschließen, daß sie von einer anderen Person als dem Empfänger gelesen wird. In einigen Fällen ist es sogar unerläßlich, daß nur der vorgesehene Empfänger und *sonst niemand* eine E-Mail liest.

Was geschieht jedoch, wenn Sie versehentlich einen falschen Buchstaben in die E-Mail-Adresse eingeben? Und was geschieht, wenn eine unbefugte Person das E-Mail-Programm eines anderen öffnet und dessen E-Mails liest?

Es gibt immer „Hacker“, also Personen, die in die Computer gelangen können, durch die E-Mails geleitet werden. Hacker können E-Mails problemlos abfangen und lesen.

Wenn Sie Ihre E-Mails verschlüsseln, können Sie sicher sein, daß sie nur von der Person gelesen werden, die den Schlüssel hat, um sie zu entschlüsseln.

Copyright © 2000 Norman

E-Mails verschlüsseln

Privacy bietet eine einfache und flexible E-Mail-Verschlüsselung für Microsoft Outlook und Exchange. Sie können folgendes verschlüsseln:

- den gesamten Inhalt Ihrer E-Mails, einschließlich der Anhänge,
- nur einen Anhang,
- nur die Nachricht oder
- nur Teile der Nachricht.

➪ ‘Eine vollständige E-Mail mit oder ohne Anhänge verschlüsseln’ auf Seite 41 und ‘Text verschlüsseln’ auf Seite 43.

E-Mails entschlüsseln

Die Entschlüsselung einer E-Mail, die mit Privacy verschlüsselt wurde, ist denkbar einfach. Wenn die gesamte E-Mail einschließlich ihrer Anhänge verschlüsselt ist, müssen Sie nur den Schlüssel zur Entschlüsselung eingeben und alles wird automatisch entschlüsselt. Für diesen Vorgang muß Privacy installiert sein.

Ist nur der Anhang als selbstentschlüsselnde Datei verschlüsselt, klicken Sie einfach doppelt darauf und geben einen Schlüssel ein. Für diesen Vorgang muß Privacy nicht installiert sein.

Wenn nur die Nachricht oder Teile der Nachricht verschlüsselt sind, entschlüsseln Sie sie mit Privacy.

➪ ‘Eine vollständige E-Mail mit oder ohne Anhänge verschlüsseln’ auf Seite 41, ‘Selbstentschlüsselnde Datei, Verzeichnis oder Datenträger entschlüsseln’ auf Seite 63, und ‘Text entschlüsseln’ auf Seite 60.

Algorithmen

Ein Algorithmus ist ein mathematisches Problemlösungsmodell, daß in ein Computerprogramm umgesetzt werden kann. Privacy verwendet bei jeder Ver- oder Entschlüsselung einen Algorithmus.

In Privacy können Sie den Algorithmus auswählen, den Sie für das Modul zur Verschlüsselung/Entschlüsselung verwenden:

- Blowfish (1.0) Ein starker, schneller und einfacher Algorithmus, der Schlüssel mit einer Länge von bis zu 448 Bit unterstützt.

Copyright © 2000 Norman

- Blowfish (2.0) Eine Modifikation von Blowfish (1.0). Wir empfehlen die Verwendung dieses Algorithmus'.
- DES (Data Encryption Standard) Ein internationalerAlgorithmus nach Regierungsstandard mit 56-Bit-Verschlüsselung.

Sicherheitsunterschiede zwischen Algorithmen

Wurden Daten mit einem Algorithmus verschlüsselt, können Sie nur mit dem Schlüssel wieder entschlüsselt werden, der auch zur Verschlüsselung verwendet wurde.

Bei manchen Algorithmen ist der Schlüssel schwieriger herauszufinden als bei anderen - je schwieriger, desto höher die Sicherheit der verschlüsselten Daten.

Der zur Zeit sicherste öffentliche Algorithmus ist Blowfish (2.0).

Private und öffentliche Schlüssel

Algorithmen können zwei Arten von Schlüsseln verwenden: private und öffentliche.

Algorithmen mit ***privaten Schlüsseln*** verwenden einen Schlüssel zum Ver- und Entschlüsseln von Informationen. ***Privacy verwendet private Schlüssel.*** Es liegt bei Ihnen, sicherzustellen, daß

- Sie den Schlüssel nur vertrauenswürdigen Personen mitteilen und
- niemand, ausgenommen dieser vertrauenswürdigen Personen, Zugang zu Ihren Schlüsseln hat.

Algorithmen mit ***öffentlichem Schlüssel*** verwenden zwei Schlüssel: einen zum Verschlüsseln, den anderen zum Entschlüsseln der Informationen. Der Schlüssel zum Verschlüsseln kann bekannt gemacht werden, da er niemals zum Entschlüsseln verwendet wird.

Sonstige Algorithmen

Sie können eine eigene .dll-Datei zum Ver- und Entschlüsseln von Daten erstellen. Einzelheiten erfahren Sie bei Norman.

➪ 'Anderen Algorithmus einstellen' auf Seite 39.

Copyright © 2000 Norman

Schlüssel und ihre Anordnung

Schlüssel

Privacy verwendet den Schlüssel zusammen mit dem Algorithmus, um Informationen zu ver- und zu entschlüsseln. Sie können beliebig viele Schlüssel erstellen.

Wenn Sie möchten, daß andere Personen Ihre Informationen entschlüsseln, teilen Sie ihnen auf sicherem Wege den Schlüssel mit, den Sie zum Verschlüsseln der Informationen verwendet haben. Mit diesem Schlüssel können sie Ihre Informationen dann entschlüsseln und gegebenenfalls an Sie gerichtete Informationen wieder verschlüsseln.

Hinweis Bei Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.

➪ ‘Schlüssel und Aliasnamen’ auf Seite 18.

Aliasnamen

Unter Privacy können Sie einen Aliasnamen mit einem Schlüssel verbinden, um ihn leichter im Gedächtnis zu behalten. Der Aliasname kann auch exportiert werden, so daß der Empfänger Ihre Daten entschlüsseln und an Sie gerichtete Daten verschlüsseln kann. Die Empfänger, denen Sie den Aliasnamen mitteilen, kennen niemals den eigentlichen Schlüssel, der mit dem Aliasnamen verbunden ist.

➪ ‘Schlüssel und Aliasnamen’ auf Seite 18.

Benutzerprofile

Benutzerprofile sind Gruppen von zusammengehörigen Aliasnamen. Sie können die Benutzerprofile in der Privacy-Datenbank auf Ihrer Workstation und Smartcard (mit NAC) speichern.

➪ ‘Benutzerprofile’ auf Seite 19.

Mehrere Benutzer können eine Kopie von Privacy verwenden. Diese Benutzer können sich dann bei Privacy anmelden und es auf der Workstation verwenden. Die einzelnen Benutzer können nicht auf die Schlüsseldetails der anderen Benutzer zugreifen.

➪ ‘Benutzer’ auf Seite 21.

Copyright © 2000 Norman

Installation

Privacy installieren

1. Schließen Sie alle aktiven Anwendungen.
2. Wenn Norman Virus Control (NVC) oder eine andere Antiviren-Software ausgeführt wird, deaktivieren Sie sie.
   Klicken Sie bei NVC mit der rechten Maustaste auf das Symbol in der Task-Leiste, klicken Sie auf **Unload** und anschließend auf **Yes**.
3. Legen Sie die Privacy-CD-ROM in das CD-ROM-Laufwerk ein.

   Ergebnis Das Privacy-Installationsfenster wird geöffnet.
4. Folgen Sie den Anweisungen des Privacy-Installationsassistenten.

   Ergebnis Privacy ist auf Ihrer Workstation installiert. Das Privacy-Fenster erscheint und zeigt die Privacy-Komponenten an, die jetzt im Windows-Startmenü verfügbar sind.
5. Klicken Sie auf die Option zur Abbildung der Readme-Datei.
6. Beende die Privacy installation, indem Sie auf **Beenden** klicken.

   Ergebnis Privacy ist jetzt installiert. Das Symbol für die **Privacy**-Verknüpfung wird auf dem Desktop angezeigt. Ein Symbol für die Zwischenablage erscheint in der Task-Leiste, die sich meist am unteren Rand Ihres Bildschirms befindet.

7. Folgen Sie der Anleitung unter ‘Anmelden’ auf Seite 13, um sich bei Privacy anzumelden.

Copyright © 2000 Norman

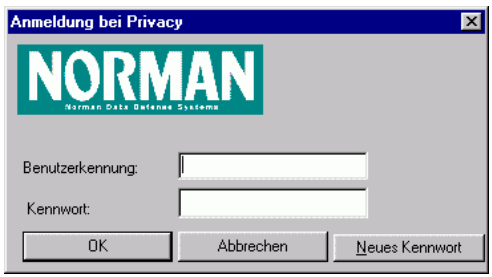
Anmelden bei Privacy

Anmelden

1 Öffnen Sie das Privacy-Anmeldedialogfeld.

➪ ‘Privacy-Dialogfeld jederzeit aufrufen’ auf Seite 15.

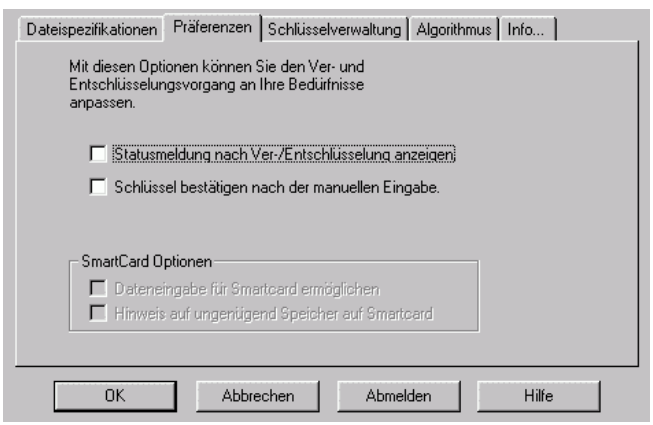
Ergebnis Folgendes Dialogfeld erscheint:



2 Geben Sie in das Feld **Benutzerkennung** die Kennung **Admin** ein.

3 Geben Sie in das Feld **Kennwort** das Kennwort **admin** ein, und klicken Sie auf **OK**.

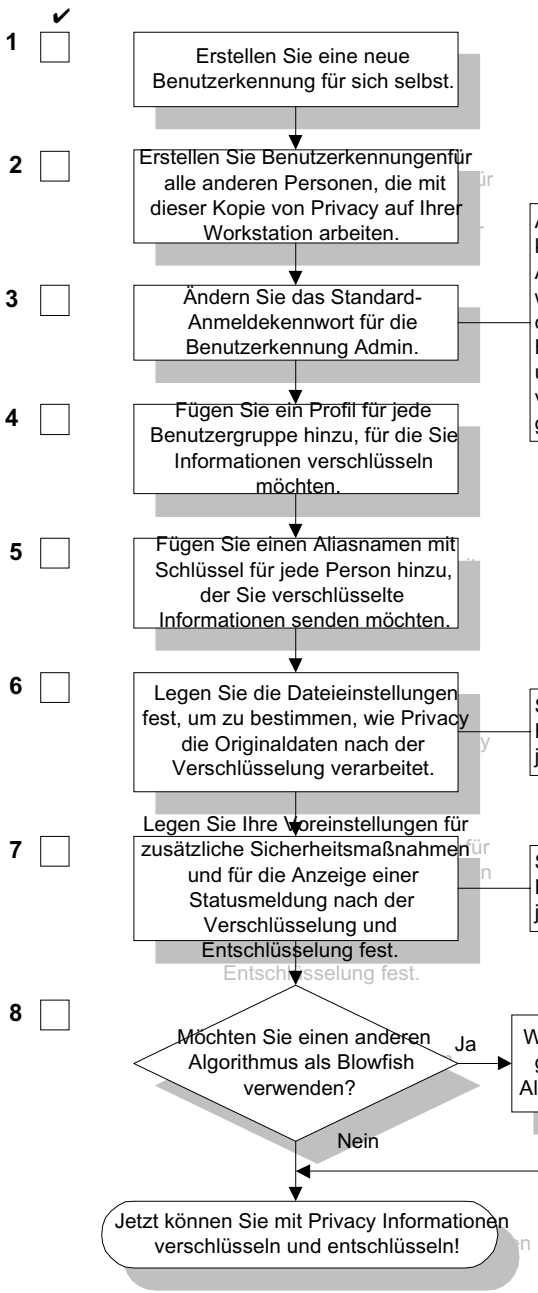
Ergebnis Das folgende Dialogfeld wird angezeigt:



➪ ‘Vorgehensweise bei der ersten Anmeldung – eine Checkliste’ auf Seite 14.

Copyright © 2000 Norman

Vorgehensweise bei der ersten Anmeldung – eine Checkliste


✔
1
Erstellen Sie eine neue Benutzerkennung für sich selbst.
2
Erstellen Sie Benutzerkennungen für alle anderen Personen, die mit dieser Kopie von Privacy auf Ihrer Workstation arbeiten.
3
Ändern Sie das Standard-Anmeldekennwort für die Benutzerkennung Admin.
Auf diese Weise können Sie die Admin-Anmeldung weiterhin verwenden, wenn Sie Ihre Benutzerkennung und Ihr Kennwort vergessen oder gelöscht haben.
4
Fügen Sie ein Profil für jede Benutzergruppe hinzu, für die Sie Informationen verschlüsseln möchten.
5
Fügen Sie einen Aliasnamen mit Schlüssel für jede Person hinzu, der Sie verschlüsselte Informationen senden möchten.
6
Legen Sie die Dateieinstellungen fest, um zu bestimmen, wie Privacy die Originaldaten nach der Verschlüsselung verarbeitet.
Sie können diese Einstellungen jederzeit ändern.
7
Legen Sie Ihre Voreinstellungen für zusätzliche Sicherheitsmaßnahmen und für die Anzeige einer Statusmeldung nach der Verschlüsselung und Entschlüsselung fest.
Sie können diese Einstellungen jederzeit ändern.
8
Möchten Sie einen anderen Algorithmus als Blowfish verwenden?
Ja
Wählen Sie den gewünschten Algorithmus aus.
Nein
Jetzt können Sie mit Privacy Informationen verschlüsseln und entschlüsseln!

Vorgehensweisen

Siehe ‘Benutzer’, page 21 und ‘Benutzerkennung hinzufügen’, page 21.

Siehe ‘Benutzer’, page 21.

Siehe ‘Anmeldekennwort ändern’, page 15.

Siehe ‘Benutzerprofile’, page 19 und ‘Benutzerprofil hinzufügen’, page 25.

Siehe ‘Schlüssel und Aliasnamen’, page 18 und ‘Aliasnamen und Schlüssel hinzufügen’, page 31.

Siehe ‘Originaldateien’, page 34.

Siehe ‘Zusätzliche Sicherheitseinstellungen’, page 36.

Siehe ‘Algorithmus für Privacy auswählen’, page 39.

Siehe ‘Verschlüsselung’, page 40 und ‘Entschlüsseln’, page 57.

Copyright © 2000 Norman

Privacy-Dialogfeld jederzeit aufrufen

Das Privacy-Dialogfeld kann auf vier verschiedene Arten aufgerufen werden, wenn Sie bei Privacy angemeldet sind, ein anderes Programm verwendet haben und dann erneut mit Privacy arbeiten möchten.

Hinweis Wenn Sie nicht bei Privacy angemeldet sind und eine der folgenden Vorgehensweisen zum Aufrufen des Privacy-Dialogfelds ausführen, wird zuerst das Privacy-Anmeldedialogfeld geöffnet.

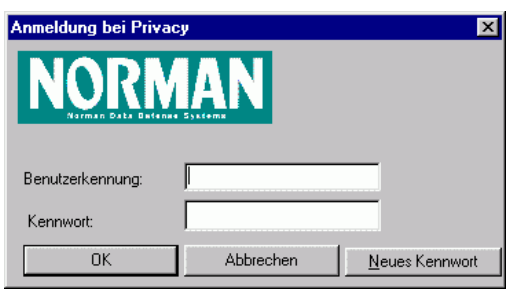
➪ ‘Anmelden’ auf Seite 13.

- Doppelklicken Sie auf dem Desktop auf das Privacy-Symbol .
- Klicken Sie in der Task-Leiste auf das Zwischenablage-Symbol und anschließend auf **Administration**.
- Klicken Sie in Ihrem E-Mail-Programm auf **Privacy-Verwaltung starten**.
- Öffnen Sie in Ihrem E-Mail-Programm eine neue E-Mail, und klicken Sie auf **Extras**, **Privacy-Verwaltung starten**.
- Klicken Sie im Menü **Start** auf **Programme**, **Norman Access Control Privacy** und dann auf **Privacy**.

Anmeldekennwort ändern

1. Stellen Sie sicher, daß Sie bei Privacy abgemeldet sind, und rufen Sie das Privacy-Anmeldedialogfeld auf.

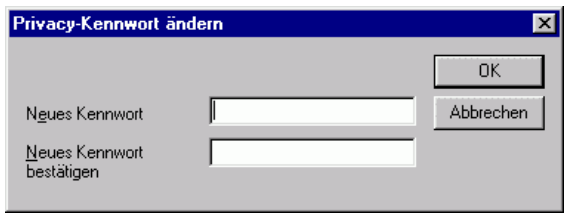
➪ ‘Privacy-Dialogfeld jederzeit aufrufen’ on page 15.



Copyright © 2000 Norman

2 Geben Sie Ihre Benutzerkennung und Ihr Anmeldekennwort ein, und klicken Sie auf **Neues Kennwort**.

Ergebnis Das folgende Dialogfeld wird angezeigt:



3 Geben Sie das neue Kennwort zweimal ein, und klicken Sie auf **OK**.
Hinweis Das Kennwort darf maximal 56 Zeichen lang sein.

Ergebnis Das Privacy-Dialogfeld wird angezeigt.

Copyright © 2000 Norman

Schlüssel erstellen

Dialogfeld Schlüsselverwaltung anzeigen

1 Öffnen Sie das Dialogfeld **Privacy**.

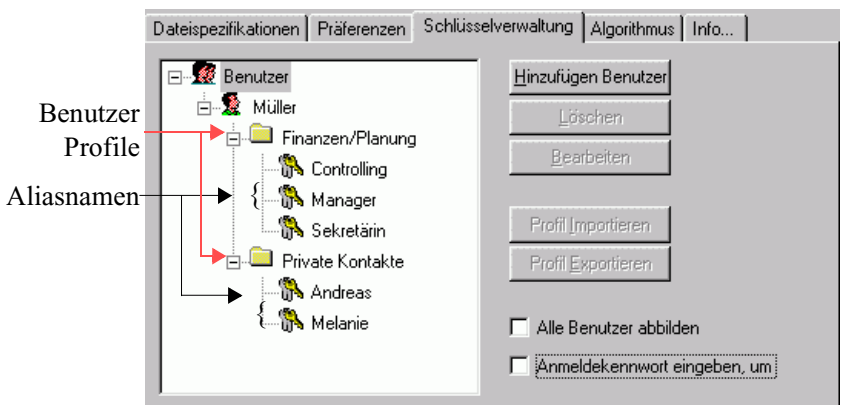
➪ ‘Privacy-Dialogfeld jederzeit aufrufen’ auf Seite 15.

2 Klicken Sie auf das Register **Schlüsselverwaltung**.

Ergebnis Das Dialogfeld **Schlüsselverwaltung** wird angezeigt.

Übersicht über das Dialogfeld Schlüsselverwaltung

Mit dem Dialogfeld **Schlüsselverwaltung** können Sie Benutzer, Profile, Aliasnamen und Schlüssel einrichten. Das folgende Beispieldialogfeld zeigt die Beziehung zwischen den verschiedenen Elementen an. Es folgt eine Beschreibung der einzelnen Elemente.



Zum Verständnis der einzelnen Elemente und ihrer Beziehungen zueinander ist es sinnvoll, sie beginnend von der untersten Ebene nach oben zu erläutern – von den Aliasnamen bis „hoch“ zu den Benutzern.

Copyright © 2000 Norman

Schlüssel und Aliasnamen

Privacy verschlüsselt und entschlüsselt Informationen mit Hilfe eines Schlüssels.

Verwenden Sie möglichst unterschiedliche Schlüssel für die Verschlüsselung folgender Elemente:

- Informationen für verschiedene Personen, zum Beispiel ein separater Schlüssel für jeden Ihrer Kollegen, Freunde u.s.w.
- Unterschiedliche Arten von Informationen, zum Beispiel separate Schlüssel für Finanzberichte und Verkaufzahlen.

Geeignete und nicht geeignete Schlüssel

Ein geeigneter Schlüssel ist „stark“, d. h. andere Benutzer können ihn nur schwer erraten. Zum Beispiel ist „3As4*^zdWy:#8SmS)a“ ein starker Schlüssel. Verwenden Sie keine einfachen oder „schwachen“ Schlüssel wie beispielsweise Ihren Namen.

Aliasnamen als Erinnerungshilfe für starke Schlüssel verwenden

Da starke Schlüssel eine komplexe Kombination von Buchstaben und Zahlen sind, ist es meist schwer, sie im Gedächtnis zu behalten. Sie können starke Schlüssel problemlos behalten und verwenden, indem Sie in Privacy einen „Aliasnamen“ erstellen, der dem Schlüssel zugeordnet wird. So können Sie dem Schlüssel „3As4*^zdWy:#“ beispielsweise den Aliasnamen „Max“ zuordnen.

Der Unterschied zwischen der Eingabe eines Schlüssels und der Auswahl eines Aliasnamens zur Verschlüsselung und Entschlüsselung

Wenn Sie einen ***Schlüssel*** verwenden, um Informationen zu verschlüsseln, geben Sie diesen einfach in das Verschlüsselungsdialogfeld ein, und Privacy verwendet Ihre Eingabe als Teil des Verschlüsselungsprozesses. Sie teilen den Schlüssel anderen Privacy-Benutzern mit, damit sie ihn in ihr jeweiliges Verschlüsselungsdialogfeld eingeben und Ihre Informationen entschlüsseln können. Diese Benutzer können diesen Schlüssel dann auch zum Verschlüsseln von Informationen verwenden, die an Sie gerichtet sind.

Copyright © 2000 Norman

Wenn Sie einen ***Aliasnamen*** zum Verschlüsseln von Informationen verwenden, geben Sie diesen nicht ein, sondern wählen ihn aus der Liste mit Aliasnamen aus, die Sie eingerichtet haben. Während des Verschlüsselungsprozesses verwendet Privacy nicht den Aliasnamen zu Verschlüsselung, sondern den Schlüssel, den Sie mit dem Aliasnamen verknüpft haben.

Damit eine andere Person die Informationen entschlüsseln kann, benötigt sie denselben Aliasnamen und Schlüssel in ihrer Privacy-Version. Dies geht am einfachsten, wenn Sie die Einzelheiten exportieren, damit andere Benutzer denselben Aliasnamen und Schlüssel einrichten können. Sie können diese Einzelheiten dann importieren – dieses Thema wird auf der nächsten Seite behandelt.

Wo Aliasnamen und Schlüssel gespeichert werden

Privacy speichert Aliasnamen und ihre dazugehörigen Schlüssel in der Datenbank Privacy.mdb auf Ihrer workstation.Sie werden als Teil eines Benutzerprofils gespeichert.

➪ Das folgende Thema ‘Benutzerprofile’.

Sicherheit für Aliasnamen und Schlüssel

Um vollständige Sicherheit für Aliasnamen und Schlüssel zu gewährleisten, verwendet Privacy Ihr Anmeldekennwort um alle Schlüssel zu verschlüsseln die sich in der Datenbank Privacy.mdb befinden.

Länge von Aliasnamen und Schlüsseln

- Aliasname kann 1 bis 255 Zeichen lang sein.
- Ein Schlüssel kann 1 bis 56 Zeichen lang sein.

➪ ‘Aliasnamen und Schlüssel hinzufügen’ auf Seite 31.

Benutzerprofile

Aliasnamen stehen oftmals in irgendeiner Form von Beziehung zueinander. Bei Privacy wird eine Gruppe zusammengehöriger Aliasnamen ***Benutzerprofil*** genannt. Mit Benutzerprofilen ist es einfach, den Aliasnamen, den Sie zum Verschlüsseln und Entschlüsseln von Informationen verwenden möchten, zu speichern und später wieder aufzufinden.

Copyright © 2000 Norman

So möchten Sie beispielsweise separate Benutzerprofile für folgendes einrichten:

- jede Abteilung in Ihrem Büro,
- jeden Abteilungsleiter,
- Ihre Familie,
- Ihre Freunde.

Privacy speichert die Profile in der Datenbank Privacy.mdb auf Ihrer workstation und/oder smartcard.

Um vollständige Sicherheit für Aliasnamen und Schlüssel zu gewährleisten, verwendet Privacy Ihr Anmeldekennwort um alle Schlüssel zu verschlüsseln, die sich in der Datenbank Privacy.mdb befinden.

Benutzerprofile exportieren und importieren

Ein Benutzerprofil ***exportieren*** Sie, damit Ihre Mitarbeiter es in Privacy ***importieren*** können. Diese können den Aliasnamen dann zur Entschlüsselung der von Ihnen gesendeten Daten und zur Verschlüsselung der Informationen an Sie verwenden.

Durch Exportieren und Importieren von Profilen brauchen Sie und Ihre Mitarbeiter die Aliasnamen und Schlüssel nicht immer wieder einzugeben. Es ist eine schnelle Methode zum Aktualisieren einer vorhandenen Datenbank.

Sicherheit beim Exportieren und Importieren

Privacy verwendet den Schlüssel, den Sie beim Exportieren des Profils eingeben, zur Verschlüsselung des Profils vor dem Exportieren. Teilen Sie den Mitarbeitern, die das Profil importieren möchten, den Schlüssel mit, den Sie zur Verschlüsselung des exportierten Profils verwendet haben. Wählen Sie dazu einen sicheren Weg in Ihrer Arbeitsumgebung, beispielsweise per Telefon oder Fax. Dadurch wird sichergestellt, daß unbefugte Benutzer die Profile nicht importieren können.

Hinweis Wenn nur ein Aliasname an eine einzige Person exportiert werden soll, legen Sie ein Benutzerprofil und einen Aliasnamen für diese Person an, z. B. ein Benutzerprofil „Abteilungsleiter“ mit dem Aliasnamen für den Abteilungsleiter.

➪ ‘Benutzerprofil hinzufügen’ auf Seite 25.

Copyright © 2000 Norman

Länge des Benutzerprofils

Der Name des profile name can be from 1 to 11 characters.
Profils kann 1 bis 255 Zeichen lang sein.

Benutzer

Privacy kann von mehreren Benutzern auf Ihrer Workstation verwendet werden. Jeder Benutzer muß jedoch über eine eigene Benutzerkennung und ein eigenes Anmeldekennwort verfügen. Im Dialogfeld für Schlüssel werden zwar alle Benutzer angezeigt, jeder Benutzer kann aber nur seine eigenen Benutzerprofile, Aliasnamen und Schlüssel ändern.

Sie können den Zugriff auf Ihre Schlüsselinformationen noch weiter eingrenzen, indem Sie eine zusätzliche Sicherheitsstufe einbauen. Dann kann nur auf das Schlüsseldialogfeld zugegriffen werden, wenn zuvor das Anmeldekennwort eingegeben wurde.

➪ ‘Benutzerkennung hinzufügen’ auf Seite 21 und ‘Zugriff auf das Dialogfeld „Schlüsselverwaltung“ einschränken’ auf Seite 38.

Länge der Benutzerkennung

- Ein Benutzerkennung kann 1 bis 255 Zeichen lang sein.
- Ein Anmeldekennwort kann 1 bis 56 Zeichen lang sein.

Benutzer

Benutzerkennung hinzufügen

Bei der Erstanmeldung bei Privacy lautet Ihr Standard-Benutzername ***Admin*** und das Standard-Anmeldekennwort ist ***admin***. Ändern Sie das Kennwort und verwenden Sie die Standardeingaben und Einzelheiten des neuen Kennworts.

Vorsicht

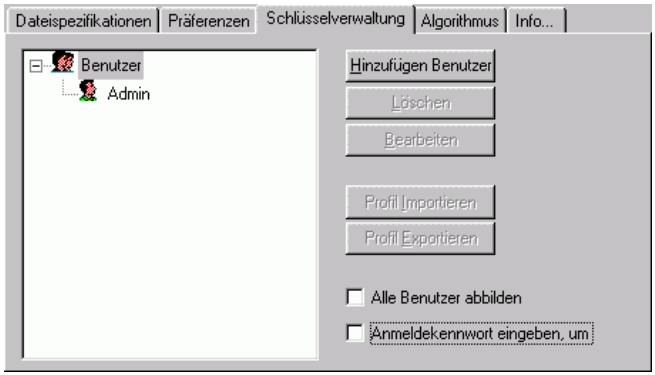
Legen Sie aus Sicherheitsgründen ***stets eine eigene Benutzerkennung und ein eigenes Anmeldekennwort fest****.*

In den folgenden Schritten wird erläutert, wie Sie eine Benutzerkennung für sich und andere Privacy-Benutzer Ihrer Workstation anlegen können.

Copyright © 2000 Norman

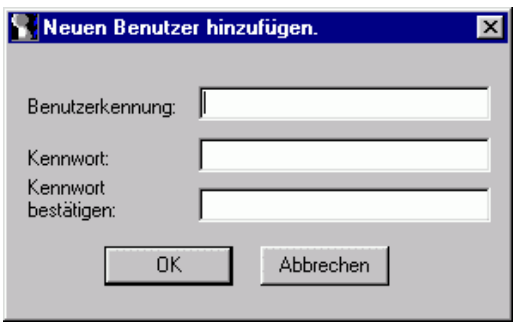
1 Rufen Sie das Dialogfeld **Schlüsselverwaltung** auf.

➪ ‘Dialogfeld Schlüsselverwaltung anzeigen’ auf Seite 17.



2 Klicken Sie auf **Benutzer** und dann auf **Neuen Benutzer hinzufügen**.

Ergebnis Folgendes Dialogfeld wird angezeigt:



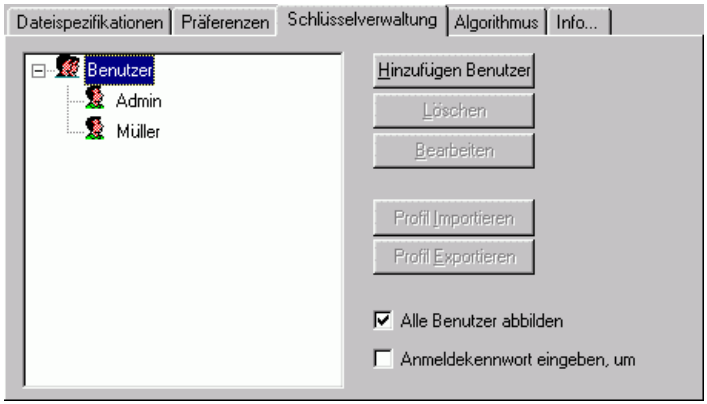
3 Geben Sie eine neue Benutzerkennung ein.

4 Geben Sie ein Anmeldekennwort ein, wiederholen Sie es, und klicken Sie auf **OK**.

Hinweis Die Benutzerkennung muß zwischen 1 und 255 Zeichen lang sein. Das Anmeldekennwort muß zwischen 1 und 56 Zeichen lang sein.

Copyright © 2000 Norman

Ergebnis Das Dialogfeld **Schlüsselverwaltung** wird erneut angezeigt. Die neue Benutzerkennung erscheint in der Liste..



5 Wenn Sie bei jedem Aufrufen des Dialogfelds **Schlüsselverwaltung** alle Benutzer in der Liste anzeigen möchten, klicken Sie auf **Alle Benutzer abbilden**.

Hinweis Obwohl jeder Anwender neue Privacy-Benutzerprofile anlegen kann, wird dem jeweiligen Benutzer das Hinzufügen und Modifizieren von Aliasnamen und Benutzerprofilen nur unter der eigenen Benutzerkennung gestattet.
Wenn Sie nicht alle Benutzer auflisten möchten, deaktivieren Sie die Option **Alle Benutzer abbilden**.

6 Von jetzt an dürfen Sie sich nur noch mit Ihrer eigenen Benutzerkennung und dem eigenen Kennwort bei Privacy anmelden. Tun Sie dies jetzt – folgen Sie dazu den Schritten 7 und 8.

7 Klicken Sie unten im Dialogfeld **Privacy** auf **Abmelden**.

8 Öffnen Sie das Privacy-Anmeldedialogfeld erneut, und melden Sie sich mit Ihrer neuen Benutzerkennung und Ihrem neuen Kennwort bei Privacy an.

➪ ‘Privacy-Dialogfeld jederzeit aufrufen’ auf Seite 15.

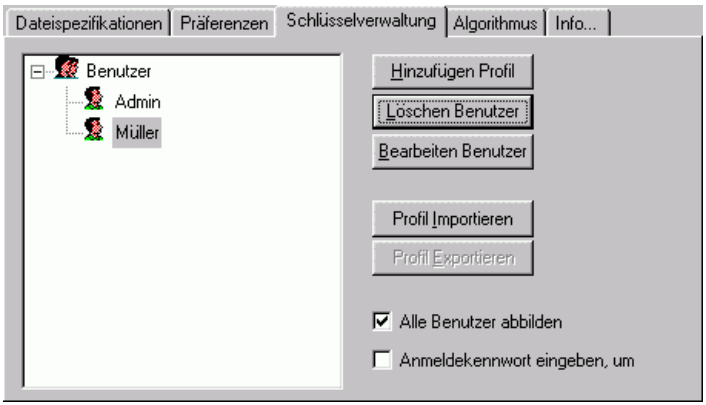
Ergebnis Mit dieser neuen Benutzerkennung können Sie nun Benutzerprofile, Aliasnamen und Schlüssel hinzufügen, ändern und löschen.

Benutzerkennung ändern

Sie können nur Ihre eigene Benutzerkennung ändern.

Copyright © 2000 Norman

1 Rufen Sie das Dialogfeld **Schlüsselverwaltung** auf:



2 Klicken Sie auf Ihre Privacy-Benutzerkennung und anschließend auf **Bearbeiten**.

Ergebnis Das Dialogfeld **Benutzerdetails bearbeiten** wird geöffnet.

3 Geben Sie Ihre neue Benutzerkennung ein, und klicken Sie auf **OK**.

Ergebnis Das Dialogfeld **Schlüsselverwaltung** wird erneut mit Ihrer neuen Benutzerkennung angezeigt.

Benutzerkennung löschen

Löschen Sie Ihren Benutzernamen nur dann, wenn Sie alle eingerichteten Profile und Aliasnamen schnell löschen wollen.

Sie können nur Ihre eigene Privacy-Benutzerkennung löschen.

1 Rufen Sie das Dialogfeld **Schlüsselverwaltung** auf.

2 Klicken Sie auf Ihre Benutzerkennung und anschließend auf **Löschen**.

Ergebnis Privacy zeigt eine Meldung an, in der Sie gefragt werden, ob Sie die Benutzerkennung mit allen Benutzerprofilen und Aliasnamen löschen möchten.

Vorsicht

Nach diesem Schritt kann der Vorgang nicht mehr rückgängig gemacht werden.

Copyright © 2000 Norman

3 Klicken Sie auf **OK**.

Ergebnis Privacy löscht die Benutzerkennung mit allen Benutzerprofilen und Aliasnamen. Anschließend wird eine Meldung angezeigt, in der Ihnen mitgeteilt wird, daß Sie jetzt abgemeldet werden.

Hinweis Wenn Sie sich wieder anmelden möchten, müssen Sie eine andere Benutzerkennung und ein anderes Kennwort verwenden.

Benutzerprofile

Benutzerprofil hinzufügen

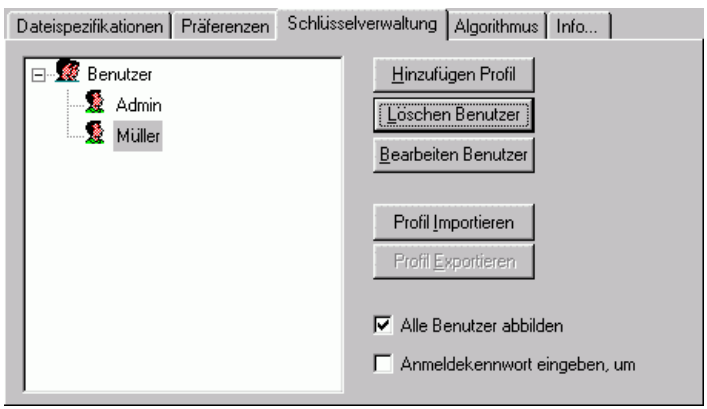
➪ Eine Übersicht über Benutzerprofile finden Sie unter ‘Benutzerprofile’ auf Seite 19.

Hinweis Sie müssen Ihre eigene Benutzerkennung hinzufügen, bevor Sie ein Profil hinzufügen können.

➪ ‘Benutzerkennung hinzufügen’ auf Seite 21.

1 Rufen Sie das Dialogfeld **Schlüsselverwaltung** auf.

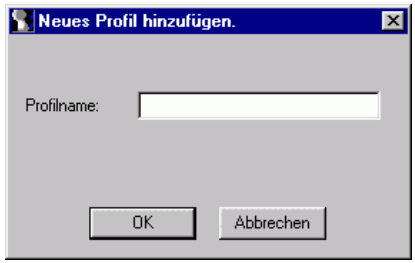
➪ ‘Dialogfeld Schlüsselverwaltung anzeigen’ auf Seite 17.



Copyright © 2000 Norman

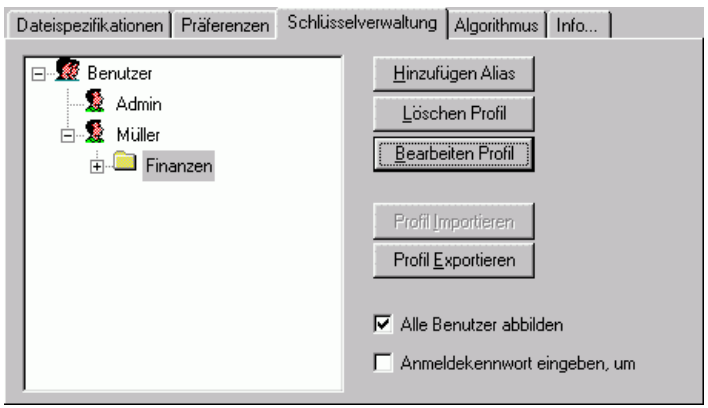
2 Klicken Sie auf Ihre Benutzerkennung und anschließend auf **Hinzufügen**.

Ergebnis Folgendes Dialogfeld wird angezeigt:



3 Geben Sie den Profilnamen ein, und klicken Sie auf **OK**.

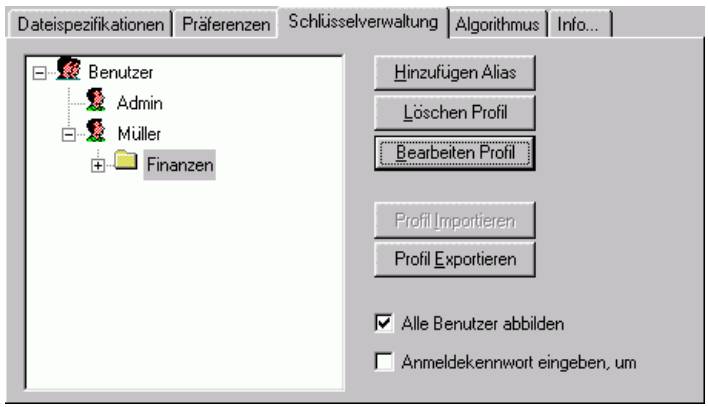
Ergebnis Das Dialogfeld **Schlüsselverwaltung** wird mit dem neuen Profilnamen erneut angezeigt.



Copyright © 2000 Norman

Benutzerprofilnamen ändern

1 Rufen Sie das Dialogfeld **Schlüsselverwaltung** auf.



2 Klicken Sie auf den Profilnamen, den Sie ändern möchten, und anschließend auf **Bearbeiten**.

Ergebnis Das Dialogfeld **Profildetails bearbeiten** wird angezeigt.

3 Geben Sie den neuen Profilnamen ein, und klicken Sie auf **OK**.

Ergebnis Das Dialogfeld **Schlüsselverwaltung** wird mit dem neuen Profilnamen erneut angezeigt.

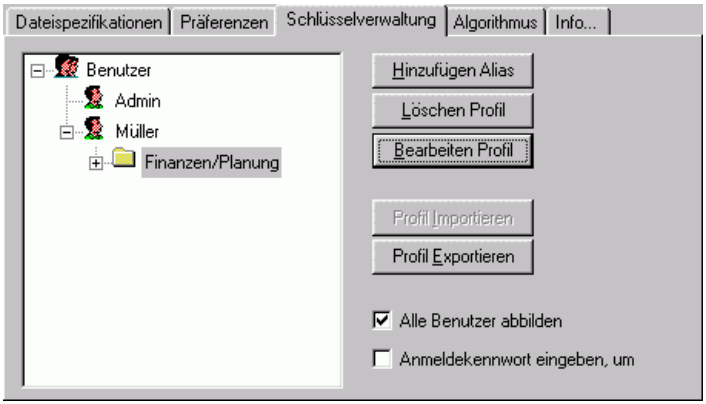
Benutzerprofil exportieren

Hinweis Ein Benutzerprofil muß mindestens einen Aliasnamen enthalten, bevor es exportiert werden kann.

➪ ‘Aliasnamen und Schlüssel hinzufügen’ auf Seite 31.

Copyright © 2000 Norman

1 Rufen Sie das Dialogfeld **Schlüsselverwaltung** auf



2 Klicken Sie auf das Profil, das Sie exportieren möchten, und anschließend auf **Profil exportieren**.

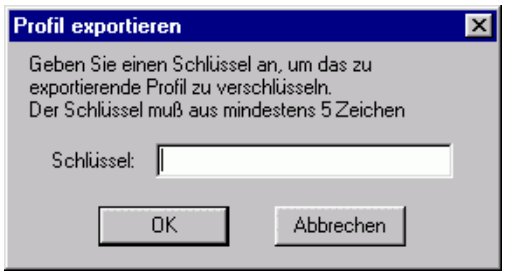
Ergebnis Das folgende Dialogfeld erscheint:

3 Wählen Sie das Verzeichnis, in dem Sie die Datei speichern möchten.

Copyright © 2000 Norman

4 Geben Sie den Namen der Exportdatei ein, und klicken Sie auf **Speichern**.

Ergebnis Das folgende Dialogfeld erscheint

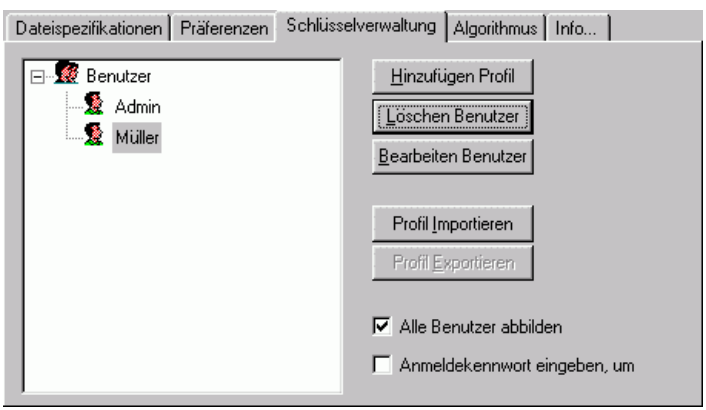

Profil exportieren
Geben Sie einen Schlüssel an, um das zu exportierende Profil zu verschlüsseln.
Der Schlüssel muß aus mindestens 5 Zeichen
Schlüssel:
OK
Abbrechen

5 Geben Sie einen Schlüssel ein, und klicken Sie auf **OK**.
Hinweis Der Schlüssel muß mindestens ***fünf*** Zeichen lang sein.

Ergebnis Privacy speichert die Details in der Datei und an der Position, die Sie angegeben haben.

Benutzerprofil importieren

1 Rufen Sie das Dialogfeld **Schlüsselverwaltung** auf.



Copyright © 2000 Norman

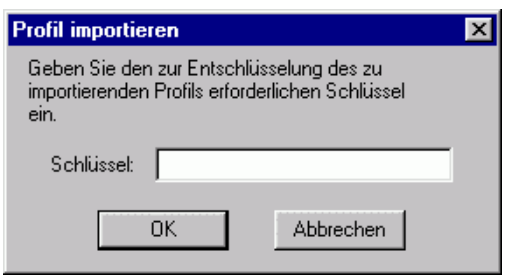
2 Klicken Sie auf Ihre Benutzerkennung und anschließend auf **Profil importieren**.

Ergebnis Das folgende Dialogfeld erscheint:

3 Wählen Sie das Verzeichnis mit der Import-datei.

4 Wählen Sie die Importdatei aus, und klicken Sie auf **Öffnen**

Ergebnis Folgendes Dialogfeld erscheint:



5 Geben Sie den zur Verschlüsselung verwendeten Schlüssel ein, und klicken Sie auf **OK**.

Ergebnis Das Dialogfeld **Schlüsselverwaltung** wird mit dem importierten Benutzerprofil unter Ihrer Benutzerkennung erneut angezeigt.

Benutzerprofil löschen

1 Rufen Sie das Dialogfeld **Schlüsselverwaltung** auf.

2 Klicken Sie auf das Profil, das Sie löschen möchten, und anschließend auf **Löschen**.

Ergebnis Privacy zeigt eine Meldung an, in der Sie gefragt werden, ob Sie sicher sind, daß Sie das Profil mit allen Aliasnamen löschen möchten.

Copyright © 2000 Norman

Vorsicht

Nach diesem Schritt kann der Vorgang nicht mehr rückgängig gemacht werden.

3 Klicken Sie auf **Löschen**.

Ergebnis Privacy löscht das Profil und alle dazugehörigen Aliasnamen und zeigt das Dialogfeld **Schlüsselverwaltung** erneut an.

Aliasnamen und Schlüssel

Aliasnamen und Schlüssel hinzufügen

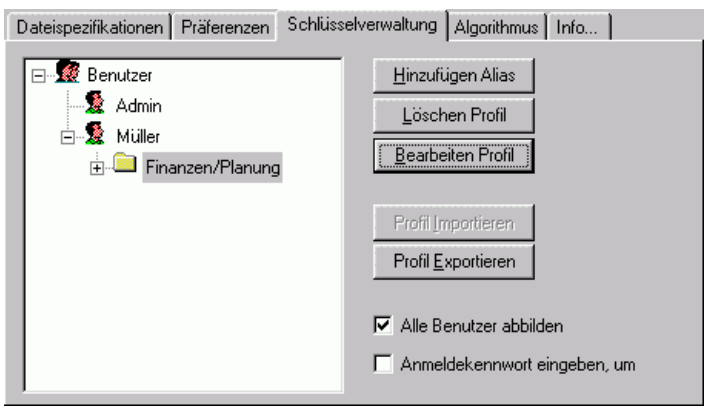
➪ Eine Übersicht über Aliasnamen und Schlüssel finden Sie unter ‘Schlüssel und Aliasnamen’ auf Seite 18.

Hinweis Sie müssen Ihre eigene Benutzerkennung und Ihr eigenes Kennwort hinzufügen, bevor Sie einen Aliasnamen und Schlüssel hinzufügen können.

➪ ‘Benutzerkennung hinzufügen’ auf Seite 21 und ‘Benutzerprofil hinzufügen’ auf Seite 25.

1 Rufen Sie das Dialogfeld **Schlüsselverwaltung** auf.

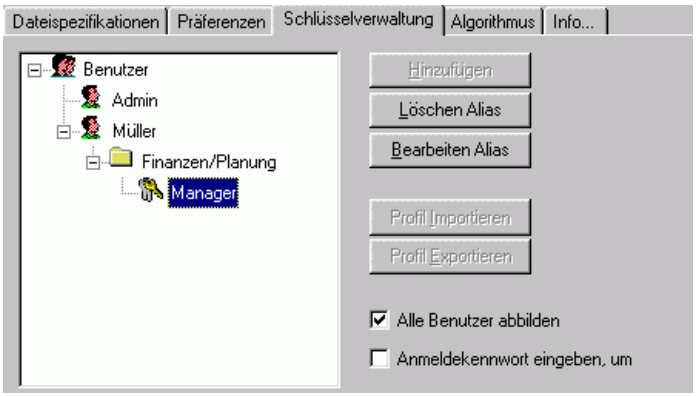
➪ ‘Dialogfeld Schlüsselverwaltung anzeigen’ auf Seite 17.



2 Klicken Sie auf das Profil, in das Sie einen neuen Aliasnamen und Schlüssel einfügen möchten, und klicken Sie anschließend auf **Hinzufügen**.

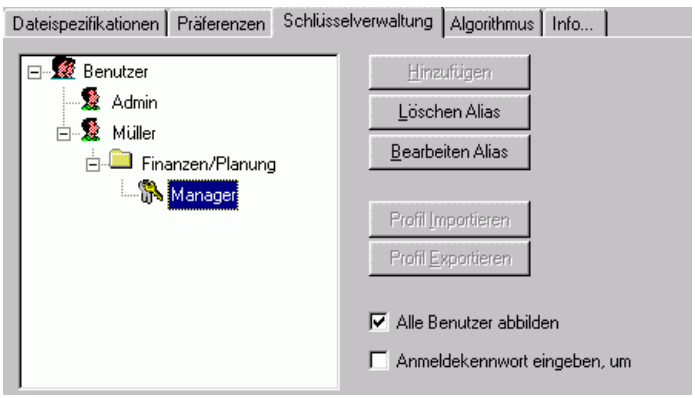
Copyright © 2000 Norman

Ergebnis Das Dialogfeld **Schlüsselverwaltung** wird mit dem gerade hinzugefügten Aliasnamen erneut angezeigt. Das folgende Dialogfeld erscheint:



Aliasnamen oder Schlüssel hinzufügen

1 Rufen Sie das Dialogfeld **Schlüsselverwaltung** auf.



2 Klicken Sie auf den Aliasnamen, für den Sie den Namen oder den Schlüssel ändern möchten, und klicken Sie auf **Bearbeiten**.

Ergebnis Das Dialogfeld **Aliasdetails bearbeiten** wird angezeigt.

3 Geben Sie den neuen Aliasnamen oder den neuen Schlüssel ein, und klicken Sie auf **OK**.

Ergebnis Das Dialogfeld **Schlüsselverwaltung** wird erneut angezeigt. Wenn Sie einen neuen Namen eingegeben haben, erscheint dieser aktualisierte Name jetzt hier.

Copyright © 2000 Norman

Aliasnamen und Schlüssel löschen

1 Rufen Sie das Dialogfeld **Schlüsselverwaltung** auf.

2 Klicken Sie auf den Aliasnamen, den Sie löschen möchten, und anschließend auf **Löschen**.

Ergebnis Privacy zeigt eine Meldung an, in der Sie gefragt werden, ob Sie sicher sind, daß Sie den Aliasnamen löschen möchten.

Vorsicht

Nach diesem Schritt kann der Vorgang nicht mehr rückgängig gemacht werden.

3 Klicken Sie auf **Ja**.

Ergebnis Privacy löscht den Aliasnamen und zeigt das Dialogfeld **Schlüsselverwaltung** erneut an.

Copyright © 2000 Norman

Originaldateien

Verarbeiten der Originaldateien

In Privacy gibt es zwei Vorgehensweisen für die Originaldateien nach dem Ver- oder Entschlüsseln:

- Speichern der Original-Zeitstempel der Datei und
- Sicheres Löschen der Datei.

Original-Zeitstempel der Dateien speichern

Wählen Sie diese Option, damit nach dem Ver- oder Entschlüsseln einer Datei die Original-Zeitstempel (erstellt, geändert und zugegriffen) und Attribute erhalten bleiben. Wenn Sie diese Option deaktivieren, ändert Privacy die Zeitstempel auf den Zeitpunkt, zu dem die Ver- oder Entschlüsselung stattfand, und gibt der Datei das Archivattribut.

➪ ‘Dateispezifikationen einstellen’ on page 35.

Originaldateien und -verzeichnisse sicher löschen

Wählen Sie diese Einstellung, damit Privacy nach dem Ver- oder Entschlüsseln einer Datei oder eines Verzeichnisses die Original-Textdatei oder das Originalverzeichnis mit von Ihnen ausgewählten Zeichen überschreibt, bevor sie gelöscht wird. (Wenn die Datei bereits verschlüsselt war, wird diese verschlüsselte Datei einfach gelöscht.) Auf diese Weise ist es sehr schwer, die Datei oder das Verzeichnis von der Festplatte wiederherzustellen.

Hinweis Privacy kann eine Datei oder ein Verzeichnis nicht löschen, wenn sie bzw. es gerade verwendet wird, zum Beispiel, wenn die Datei gerade in einem Textverarbeitungsprogramm geöffnet ist.

➪ ‘Dateispezifikationen einstellen’ on page 35.

Copyright © 2000 Norman

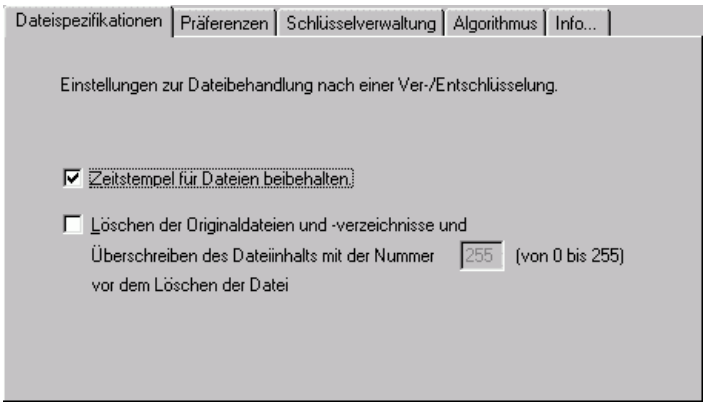
Dateispezifikationen einstellen

1 Rufen Sie das Dialogfeld **Privacy** auf.

➪ 'Privacy-Dialogfeld jederzeit aufrufen' auf Seite 15.

2 Klicken Sie auf das Register **Dateispezifikationen**.

Ergebnis Das folgende Dialogfeld wird angezeigt:



3 Klicken Sie auf eine oder mehrere Einstellungen. (Sie werden auf der vorhergehenden Seite beschrieben.)

4 Wenn Sie die Option zum sicheren Löschen der Originaldateien und -verzeichnisse ausgewählt haben, lassen Sie entweder die Standardanzahl der überschriebenen Zeichen bei 255 (wird im Feld angezeigt), oder geben Sie Ihre gewünschte Anzahl ein.

Ergebnis Bevor Privacy die Datei oder das Verzeichnis löscht, werden die Daten mit der von Ihnen ausgewählten Zeichenanzahl überschrieben.
Privacy wendet Ihre Einstellungen jetzt auf alle zukünftigen ver- und entschlüsselten Dateien und Verzeichnisse an.

5 Klicken Sie auf **OK**.

Copyright © 2000 Norman

Zusätzliche Sicherheitseinstellungen

Zusätzliche Sicherheitseinstellungen

Es gibt zwei zusätzliche Sicherheitseinstellungen:

- Schlüssel nach der manuellen Eingabe bestätigen.
- Anmeldekennwort eingeben, um das Dialogfeld **Schlüsselverwaltung** aufzurufen.

Schlüssel nach der manuellen Eingabe bestätigen

Wählen Sie diese Einstellung immer dann, wenn Sie manuell einen Schlüssel zum Ver- oder Entschlüsseln von Informationen eingeben. Auf diese Weise können Sie den Schlüssel leichter im Gedächtnis behalten.

➪ ‘Voreinstellungen vornehmen’ auf Seite 37.

Anmeldekennwort eingeben, um das Dialogfeld „Schlüsselverwaltung“ aufzurufen

Verwenden Sie diese Option, damit nur die Personen auf das Dialogfeld **Schlüsselverwaltung** zugreifen können, die das Anmeldekennwort für Privacy kennen.

Wenn Sie Ihre Workstation verlassen, stellen Sie zuvor sicher, daß Sie auf ein beliebiges Register, ausgenommen des Registers **Schlüsselverwaltung,** klicken. Auf diese Weise kann ein Unbefugter, der in Ihrer Abwesenheit auf Ihre Schlüsselinformationen zugreifen möchte, dies nicht ohne Ihr Anmeldekennwort tun.

➪ ‘Zugriff auf das Dialogfeld „Schlüsselverwaltung“ einschränken’ auf Seite 38.

Copyright © 2000 Norman

Zusätzliche Informationen

Im Dialogfeld **Präferenzen** gibt es eine Option zum Anzeigen einer Statusmeldung nach der Ver- oder Entschlüsselung. Wählen Sie diese Einstellung, wenn Sie möchten, daß nach der Ver- oder Entschlüsselung von Informationen eine Bestätigungsmeldung angezeigt wird.

Smartcard-Optionen

Diese Optionen sind nur dann verfügbar, wenn Sie Privacy zusammen mit dem Programm Norman Access Control (NAC) für Windows 95/98, NAC für NT oder NAC für Notebooks verwenden.

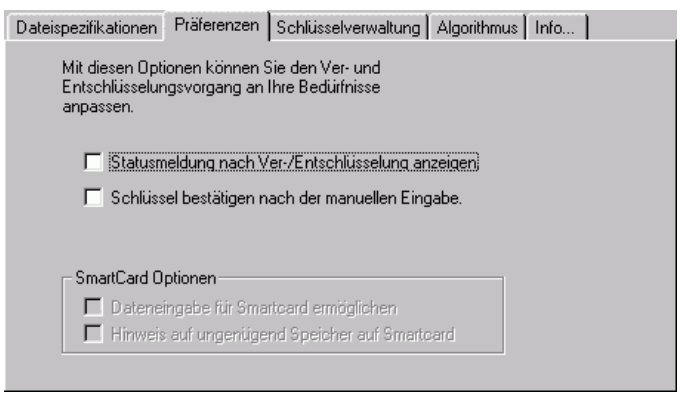
Voreinstellungen vornehmen

1 Öffnen Sie das Dialogfeld **Privacy**.

➪ ‘Privacy-Dialogfeld jederzeit aufrufen’ auf Seite 15.

2 Klicken Sie auf das Register **Präferenzen**.

Ergebnis Das folgende Dialogfeld erscheint:



Copyright © 2000 Norman

3 Klicken Sie auf eine oder mehrere Einstellungen und anschließend auf **OK**. (Die Einstellungen werden auf der vorhergehenden Seite beschrieben.)

Ergebnis Privacy wendet die Einstellungen auf alle zukünftig ver- und entschlüsselten Informationen an.

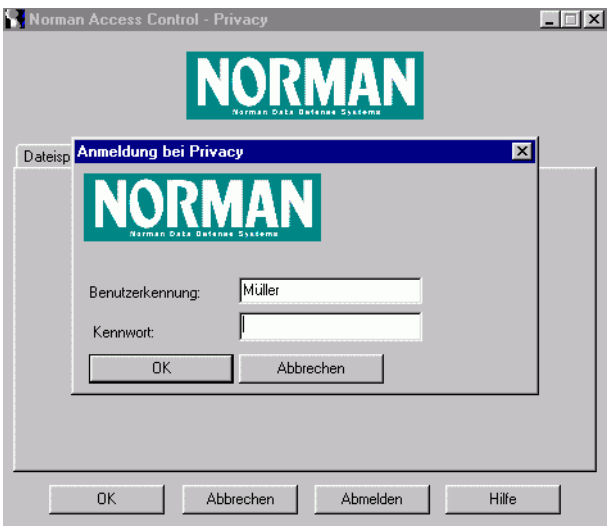
Zugriff auf das Dialogfeld „Schlüsselverwaltung“ einschränken

1 Öffnen Sie das Dialogfeld **Schlüsselverwaltung**.

➪ ‘Dialogfeld Schlüsselverwaltung anzeigen’ auf Seite 17.

2 Klicken Sie in der unteren rechten Ecke des Dialogfelds auf **Anmeldeschlüssel eingeben, um das Dialogfeld „Schlüsselverwaltung“ zu öffnen.** Klicken Sie anschließend auf **OK**.

Ergebnis Beim nächsten Öffnen des Dialogfelds **Schlüsselverwaltung** fragt Privacy Sie zuvor nach Ihrem Anmeldekennwort.



Copyright © 2000 Norman

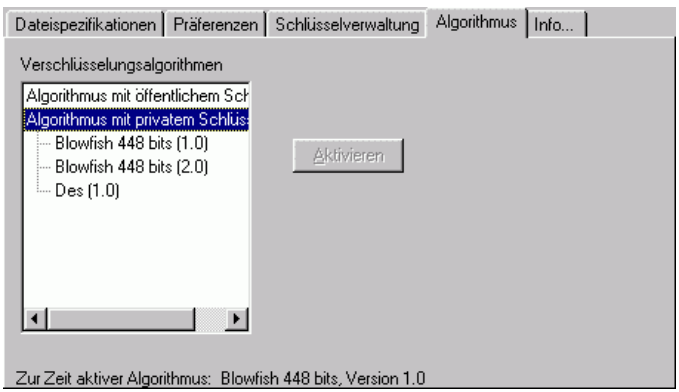
Privacy-Algorithmen

➪ Eine Übersicht über Algorithmen finden Sie unter ‘Algorithmen’ auf Seite 9.

Algorithmus für Privacy auswählen

1 Klicken Sie im Dialogfeld **Privacy** auf das Register **Algorithmen**.

Ergebnis Das folgende Dialogfeld wird angezeigt:



2 Klicken Sie in der Liste der Verschlüsselungsalgorithmen auf den Algorithmus, mit dem Privacy Ihre Informationen verschlüsseln und entschlüsseln soll. Klicken Sie anschließend auf **Aktivieren**.

Ergebnis Privacy verwendet diesen Algorithmus jetzt für alle Verschlüsselungsvorgänge.

Anderen Algorithmus einstellen

Sie können auch Ihren eigenen Algorithmus für Privacy einstellen. Bitte wenden Sie sich an Norman, um weitere Einzelheiten dazu zu erfahren. Die Kontaktadressen finden Sie auf Seite iii.

Copyright © 2000 Norman

Verschlüsselung

Dialogfeld Schlüsselwahl

Wenn Sie Informationen verschlüsseln, tun Sie dies, indem Sie einen Schlüssel eingeben oder einen Aliasnamen auswählen, für den Privacy dann den zugehörigen Schlüssel einfügt.

In Privacy können Sie den gewünschten Aliasnamen auswählen.

1 Klicken Sie dazu in einem beliebigen Privacy-Verschlüsselungsdialogfeld auf **Suchen** neben dem Feld **Schlüssel**.

Ergebnis Das Dialogfeld **Schlüsselwahl** wird mit Ihren Benutzerprofilen und Aliasnamen angezeigt.

2 Doppelklicken Sie auf den Aliasnamen, dessen Schlüssel Sie aufrufen möchten.

Ergebnis Privacy fügt den Schlüssel in das Feld **Schlüssel** ein.

Copyright © 2000 Norman

Eine vollständige E-Mail mit oder ohne Anhänge verschlüsseln

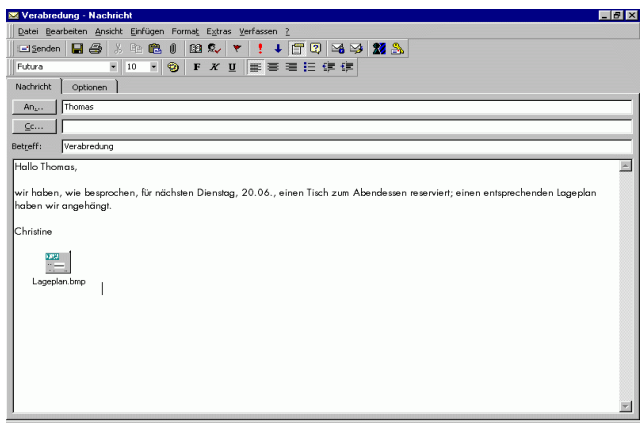
➪ Eine Übersicht über die Verschlüsselung von E-Mails finden Sie unter ‘E-Mails verschlüsseln und entschlüsseln’ auf Seite 8.

1 Erstellen Sie eine neue E-Mail. Hängen Sie alle Dateien an, die Sie mit der E-Mail senden möchten.

Hinweis Sie können unverschlüsselte oder verschlüsselte Dateien anhängen. Wenn Sie die E-Mail senden, verschlüsselt Privacy verschlüsselte Dateien erneut.
Wenn Sie den Anhang komprimieren oder mit einem Ablaufdatum versehen möchten, müssen Sie die Datei verschlüsseln, bevor Sie sie an E-Mail anhängen.

➪ Die Themen zum Verschlüsseln einer Datei, eines Verzeichnisses oder Datenträgers in diesem Abschnitt.

Ergebnis Ihre E-Mail sieht ähnlich aus wie hier



2 Wenn Sie einen neuen Aliasnamen für die Person erstellen möchten, an die Sie die E-Mail senden, oder Privacy vor dem Versenden der E-Mail konfigurieren möchten, klicken Sie auf **Privacy-Administration starten**.

Ergebnis Das Privacy-Dialogfeld **Präferenzen** wird angezeigt.

➪ ‘Schlüssel erstellen’ auf Seite 17, ‘Verarbeiten der Originaldateien’ auf Seite 34 und ‘Zusätzliche Sicherheitseinstellungen’ auf Seite 36.

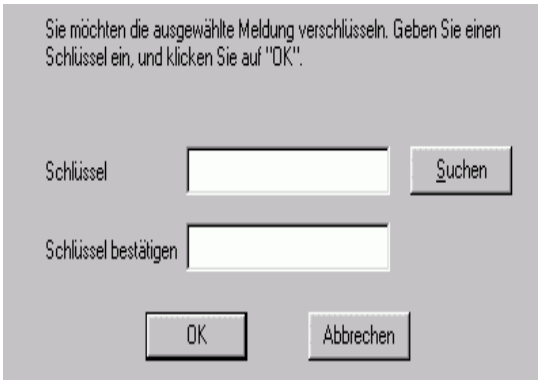
Copyright © 2000 Norman

3 Entweder

- klicken Sie auf **Beim Senden verschlüsseln** ***oder***
- klicken Sie auf **Extras**, **Verschlüsseln beim Senden**.

4 Klicken Sie auf **Senden**.

Ergebnis Das folgende Dialogfeld erscheint:



5 Geben Sie einen Schlüssel ein, oder klicken Sie auf S**uchen**, und doppelklicken Sie im Dialogfeld **Schlüsselwahl** auf einen Aliasnamen.

Hinweis Geben Sie den Aliasnamen nicht in das Feld **Schlüssel** ein. Wenn Sie den Schlüssel eines Aliasnamens verwenden möchten, müssen Sie den Aliasnamen im Dialogfeld **Schlüsselwahl** auswählen.

Ergebnis Privacy zeigt Sternchen (*) im Feld **Schlüssel** an.

6 Klicken Sie auf **OK**.

Ergebnis Privacy verschlüsselt den Text der E-Mail und ihrer Anhänge, und sendet die E-Mail anschließend an den Empfänger.

Hinweis Privacy verwirft alle Textformatierungen, zum Beispiel fett oder kursiv gedruckten Text.

Copyright © 2000 Norman

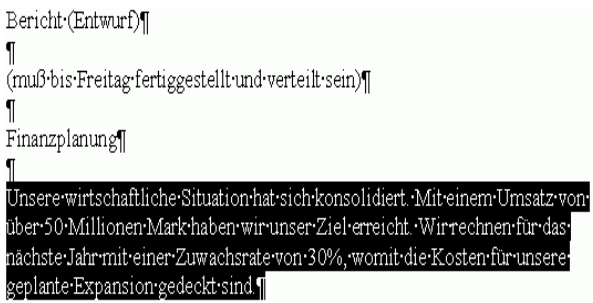
Text verschlüsseln

➪ Informationen über das Verschlüsseln von Text finden Sie unter ‘Text schützen’ auf Seite 7.

Hinweis Diese Methode gilt für die Verschlüsselung von ***reinem Text*** einschließlich Buchstaben, Zahlen und Symbolen bis zu 2 MB. Bei der Verschlüsselung von Bildern oder Grafiken muß die gesamte Datei, in der sie sich befinden, verschlüsselt werden. Beachten Sie ebenfalls, daß beim Verschlüsseln von Text sämtliche Formatierungen verlorengehen.

➪ ‘Datei verschlüsseln – Standard’ auf Seite 45 oder ‘Datei verschlüsseln – selbstentschlüsselnd’ auf Seite 47.

1 Wählen Sie den Text aus, den Sie verschlüsseln möchten.

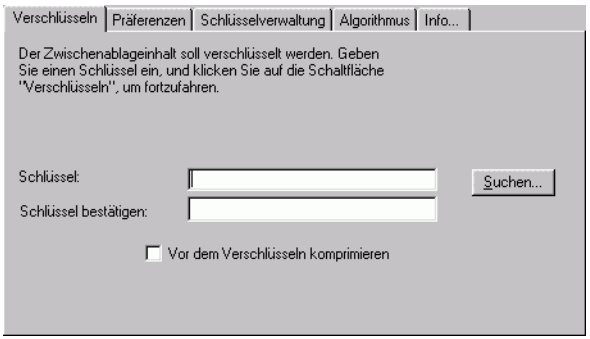


2 Kopieren Sie den Text in die Zwischenablage. Drücken Sie dazu beispielsweise
Strg + C.

3 Klicken Sie auf das Zwischenablage-Symbol in der Task-Leiste und anschließend auf **Zwischenablage verschlüsseln**.

Ergebnis Wenn Sie nicht angemeldet sind, wird das Privacy-Anmeldedialogfeld angezeigt, und Sie melden sich an. Nach der Anmeldung, oder wenn Sie bereits angemeldet sind, erscheint folgendes Dialogfeld:

Copyright © 2000 Norman



4 Geben Sie einen Schlüssel ein, oder klicken Sie auf **Suchen**, und doppelklicken Sie im Dialogfeld **Schlüsselwahl** auf einen Aliasnamen.

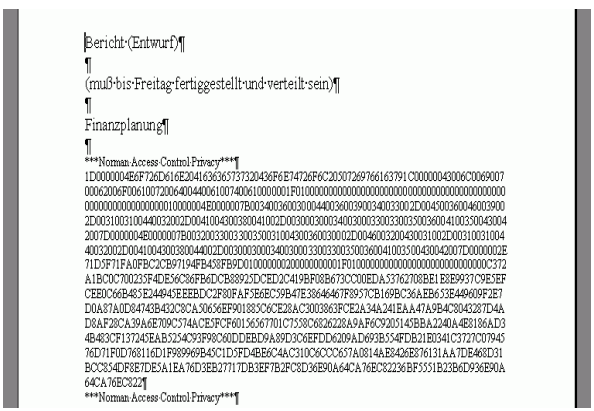
Hinweis Geben Sie keinen Aliasnamen in das Feld **Schlüssel** ein. Wenn Sie den Schlüssel eines Aliasnamens verwenden möchten, müssen Sie den Aliasnamen im Dialogfeld **Schlüsselwahl** auswählen.

5 Wenn Sie den Text komprimieren möchten, klicken Sie auf **Vor dem Verschlüsseln komprimieren**.

6 Klicken Sie auf **Verschlüsseln**.

7 Fügen Sie den Inhalt der Zwischenablage (den verschlüsselten Text) über dem markierten Text ein. Drücken Sie dazu zum Beispiel **Strg + V**.

Ergebnis Der verschlüsselte Text sieht folgendermaßen aus:


Bericht·(Entwurf)¶
¶
(muß·bis·Freitag·fertiggestellt·und·verteilt·sein)¶
¶
Finanzplanung¶
¶
Norman·Access·Control·Privacy¶
1D0000004E6F726D616E20416363673732036F6E74726F6C20507269766163791C0000004300600690070006200600610072006400440061007400610000001F01000000000

Datei verschlüsseln – Standard

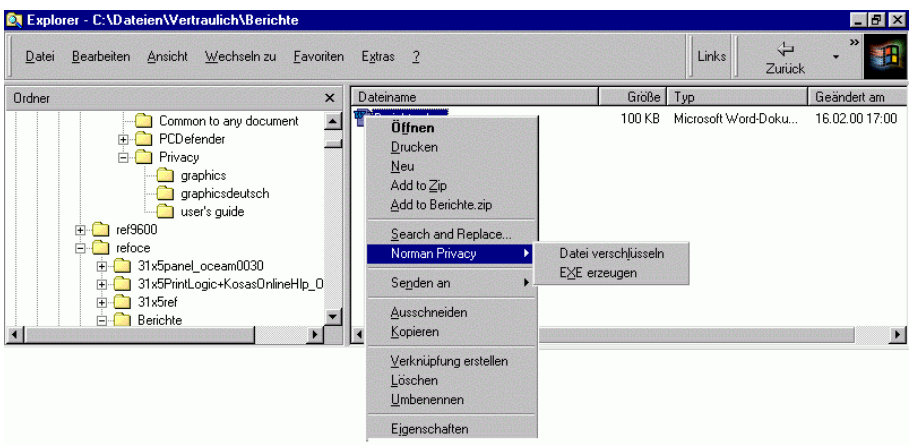
➪ Eine Übersicht über die Verschlüsselung von Dateien finden Sie unter ‘Informationen in Dateien schützen’ auf Seite 6.

1 Gehen Sie im Windows Explorer oder in einem seiner Dialogfelder (Speichern, Speichern unter, Öffnen oder Suchen) folgendermaßen vor:

- ziehen Sie die Datei auf das Desktop-Symbol für **Privacy**

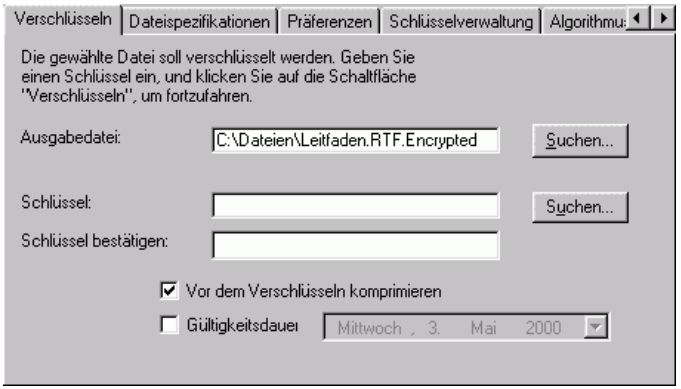
  , ***oder***

- klicken Sie mit der rechten Maustaste auf die Datei, die Sie verschlüsseln möchten, klicken Sie auf Norman Privacy und dann auf **Datei verschlüsseln** (siehe unten)



Ergebnis Das Dialogfeld **Verschlüsseln** erscheint und zeigt den ausgewählten Dateinamen mit der Erweiterung *Encrypted* (verschlüsselt) an.

Copyright © 2000 Norman



Hinweis Wenn Sie sich entscheiden, daß Sie eine andere Datei verschlüsseln möchten, ziehen Sie die Datei einfach aus dem Windows Explorer, und legen Sie sie auf dem Privacy-Dialogfeld ab. Der Name der **Ausgabedatei** ändert sich automatisch.

2 Behalten Sie entweder den vollen Dateinamen bei, geben Sie einen neuen Dateinamen in das Feld **Ausgabedatei** ein, oder klicken Sie auf **Suchen**, und wählen Sie einen Dateinamen aus.

3 Geben Sie einen Schlüssel ein, oder klicken Sie auf **Suchen** neben dem Feld **Schlüssel** und doppelklicken Sie im Dialogfeld **Schlüsselwahl** auf einen Aliasnamen.

Hinweis Geben Sie keinen Aliasnamen in das Feld **Schlüssel** ein. Wenn Sie den Schlüssel eines Aliasnamens verwenden möchten, müssen Sie den Aliasnamen im Dialogfeld **Schlüsselwahl** auswählen.

Ergebnis Privacy zeigt Sternchen (*) im Dialogfeld **Schlüssel** an.

4 Wenn Sie die Datei ***nicht*** komprimieren möchten, deaktivieren Sie die Option **Vor dem Verschlüsseln komprimieren**.

5 Wenn Sie ***kein*** Ablaufdatum festlegen möchten, zu dem der verschlüsselte Text nicht mehr zugänglich ist, ***fahren Sie mit*** Schritt 7 ***fort***.

Wenn Sie ein Ablaufdatum festlegen ***möchten***, klicken Sie auf **Gültigkeitsdauer** und dann auf den Pfeil neben dem Datum.

Copyright © 2000 Norman

Ergebnis Das folgende Dialogfeld erscheint mit dem aktuellen Datum eingekreist

6 Klicken Sie auf das Datum, zu dem die Datei ablaufen soll. Wenn Sie ein Datum im Feld **Gültigkeitsdauer** ändern möchten, klicken Sie auf den entsprechenden Tag, Monat oder das Jahr, und verwenden Sie die Pfeiltasten.

Ergebnis Das Dialogfeld **Verschlüsseln** wird erneut angezeigt.

7 Legen Sie fest, wie die Originaldatei verarbeitet werden soll.

➪ ‘Originaldateien’ auf Seite 34.

8 Legen Sie gegebenenfalls zusätzliche Sicherheits- und Informationseinstellungen fest.

➪ ‘Zusätzliche Sicherheitseinstellungen’ auf Seite 36.

9 Haben Sie diesen Vorgang ausgehend vom Abschnitt ‘Datei verschlüsseln – selbstentschlüsselnd’ auf Seite 47 gelesen?
Ja Fahren Sie mit Schritt 3 in dem Vorgang fort.
Nein Fahren Sie mit Schritt 10 fort.

10 Klicken Sie auf **Verschlüsseln**.

Ergebnis Privacy verschlüsselt die Datei. Sie erscheint im Explorer unter dem Namen *Ihrdateiname.dateityp.Encrypted*.
Zum Beispiel *StyleGuide.doc.Encrypted*.

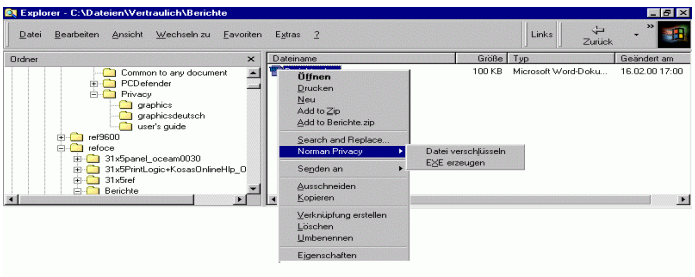
Datei verschlüsseln – selbstentschlüsselnd

➪ Eine Übersicht über die Verschlüsselung von Dateien finden Sie unter ‘Informationen in Dateien schützen’ auf Seite 6.

1 Klicken Sie im Windows Explorer oder in einem seiner Dialogfelder (Speichern, Speichern unter, Öffnen oder Suchen) mit der rechten Maustaste auf die Datei, für die Sie eine selbstentschlüsselnde Datei

Copyright © 2000 Norman

anlegen möchten, klicken Sie auf **Norman Privacy** und dann auf **EXE erzeugen**.



Ergebnis Ist die ***Datei bereits verschlüsselt***, erstellt Privacy die selbstentschlüsselnde Datei. Die Datei erscheint im Explorer unter dem Namen *ihrdateiname.Encrypted.exe*. **Ende des Vorgangs**. Ist die ***Datei nicht verschlüsselt***, wird das Privacy-Verschlüsselungsdialogfeld mit dem ausgewählten Dateinamen und der Erweiterung *Encrypted* angezeigt.

2 Gehen Sie zum Abschnitt ‘Datei verschlüsseln – Standard’ auf Seite 45, Schritt 2. Folgen Sie diesem Vorgang, bis Sie angewiesen werden, hierher zurückzukehren.

3 Klicken Sie auf **Verschlüsseln**.

Ergebnis Privacy verschlüsselt die Datei und erstellt unmittelbar danach die selbstentschlüsselnde Datei. Die Datei erscheint im Explorer unter dem Namen *ihrdateiname.dateityp.Encrypted.exe*.

Verzeichnis verschlüsseln – Standard

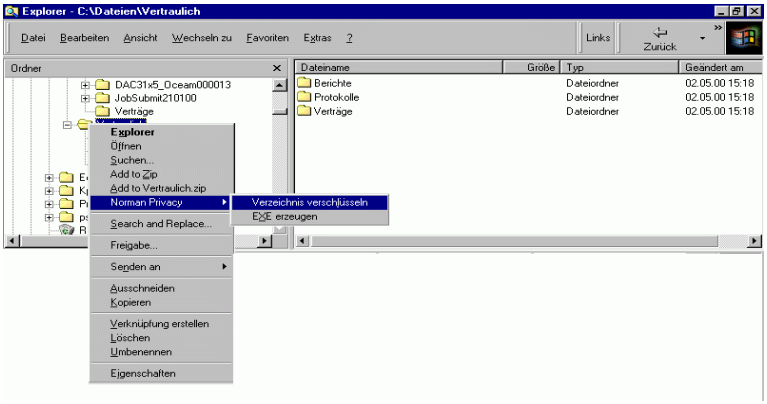
➪ Eine Übersicht über die Verschlüsselung von Verzeichnissen finden Sie unter ‘Informationen in Verzeichnissen schützen’ auf Seite 6.

1 Gehen Sie im Windows Explorer oder einem seiner Dialogfelder (Speichern, Speichern unter, Öffnen oder Suchen) folgendermaßen vor:

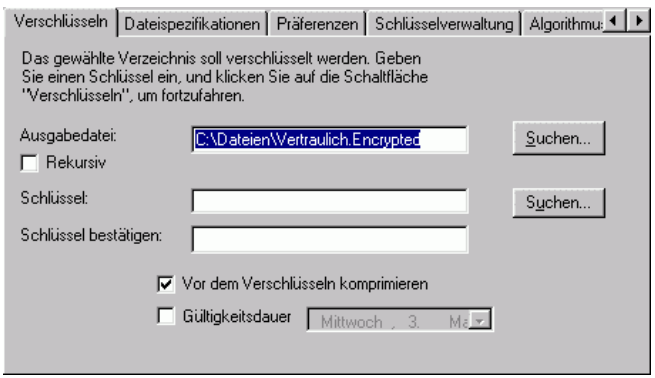
- ziehen Sie das Verzeichnis auf das Desktop-Symbol für **Privacy** , ***oder***

Copyright © 2000 Norman

- klicken Sie mit der rechten Maustaste auf das Verzeichnis, das Sie verschlüsseln möchten, klicken Sie auf **Norman Privacy** und anschließend auf **Verzeichnis verschlüsseln** (siehe unten)



Ergebnis Das folgende Dialogfeld wird angezeigt:



Hinweis Wenn Sie sich entscheiden, daß Sie ein anderes Verzeichnis verschlüsseln möchten, ziehen Sie das Verzeichnis einfach aus dem Windows Explorer, und legen Sie es auf dem Privacy-Dialogfeld ab. Der Name des **Ausgabeverzeichnisses** ändert sich automatisch.

2 Behalten Sie entweder den Standardnamen für die Ausgabedatei bei, geben Sie einen neuen Dateinamen in das Feld **Ausgabedatei** ein, oder klicken Sie auf **Suchen**, und wählen Sie einen Dateinamen aus.

3 Wenn Sie alle Daten in den Unterverzeichnissen des ausgewählten Verzeichnisses verschlüsseln möchten, klicken Sie auf **Rekursiv**.

Copyright © 2000 Norman

4 Geben Sie einen Schlüssel ein, oder klicken Sie auf **Suchen** neben dem Feld **Schlüssel**, und doppelklicken Sie auf einen Aliasnamen im Dialogfeld **Schlüsselwahl**.

Hinweis Geben Sie keinen Aliasnamen in das Feld **Schlüssel** ein. Wenn Sie den Schlüssel eines Aliasnamens verwenden möchten, müssen Sie den Aliasnamen im Dialogfeld **Schlüsselwahl** auswählen.

Ergebnis Privacy zeigt Sternchen (*) im Dialogfeld **Schlüssel** an.

5 Wenn Sie das Verzeichnis ***nicht*** komprimieren möchten, deaktivieren Sie die Option **Vor dem Verschlüsseln komprimieren**.

6 Wenn Sie ***kein*** Ablaufdatum festlegen möchten, zu dem der verschlüsselte Text nicht mehr zugänglich ist, ***fahren Sie mit*** Schritt 8 ***fort***.

Wenn Sie ein Ablaufdatum festlegen ***möchten***, klicken Sie auf **Gültigkeitsdauer** und dann auf den Pfeil neben dem Datum.

Ergebnis Das folgende Dialogfeld erscheint mit dem aktuellen Datum eingekreist:

7 Klicken Sie auf das Datum, zu dem die Datei ablaufen soll. Wenn Sie ein Datum im Feld **Gültigkeitsdauer** ändern möchten, klicken Sie auf den entsprechenden Tag, Monat oder das Jahr, und verwenden Sie die Pfeiltasten.

Ergebnis Das Dialogfeld **Verschlüsseln** wird erneut angezeigt.

8 Legen Sie fest, wie die Originaldatei verarbeitet werden soll.

➪ ‘Originaldateien’ auf Seite 34.

9 Legen Sie gegebenenfalls zusätzliche Sicherheits- und Informationseinstellungen fest.

➪ ‘Zusätzliche Sicherheitseinstellungen’ auf Seite 36.

Copyright © 2000 Norman

10 Haben Sie diesen Vorgang ausgehend vom Abschnitt ‘Verzeichnis verschlüsseln – selbstentschlüsselnd’ auf Seite 51 gelesen?
Ja Fahren Sie mit Schritt 3 in diesem Vorgang fort.
Nein Fahren Sie mit Schritt 11 fort.

11 Klicken Sie auf **Verschlüsseln**.

Ergebnis Privacy verschlüsselt das Verzeichnis und legt alle Unterverzeichnisse in einer verschlüsselten ***Datei*** namens *ihrverzeichnisname.Encrypted* ab.

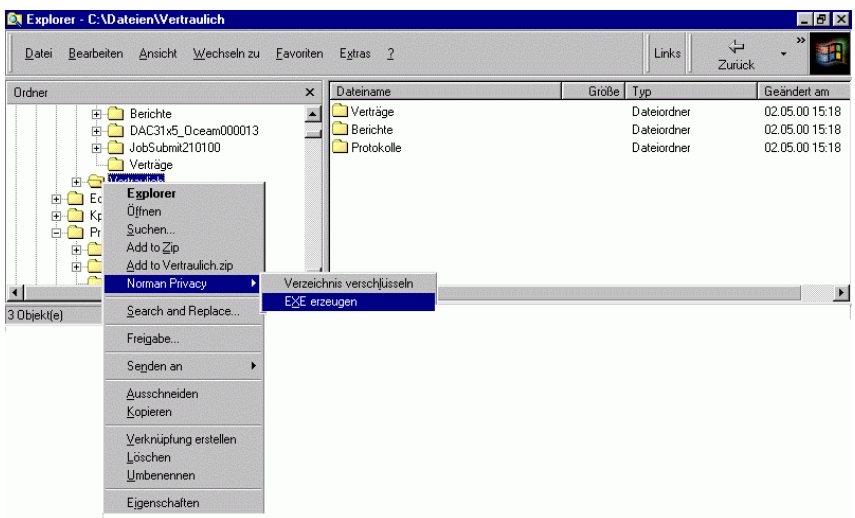
Verzeichnis verschlüsseln – selbstentschlüsselnd

➪ Eine Übersicht über die Verschlüsselung von Verzeichnissen finden Sie unter ‘Informationen in Verzeichnissen schützen’ auf Seite 6.

Hinweis Wenn das Verzeichnis bereits verschlüsselt ist, erscheint es im Explorer als eine verschlüsselte ***Datei***.

➪ ‘Datei verschlüsseln – selbstentschlüsselnd’ auf Seite 47.

1 Klicken Sie im Windows Explorer oder in einem seiner Dialogfelder (Speichern, Speichern unter, Öffnen oder Suchen) mit der rechten Maustaste auf das Verzeichnis, für das Sie eine selbstentschlüsselnde Datei anlegen möchten, klicken Sie auf **Norman Privacy** und dann auf **EXE erzeugen**.



Copyright © 2000 Norman

Ergebnis Das Privacy-Verschlüsselungsdialogfeld wird mit dem ausgewählten Verzeichnisnamen und der Erweiterung *Encrypted* angezeigt.

Hinweis Dieses Dialogfeld enthält eine „Ausgabedatei“, weil der Inhalt des Verzeichnisses zum Schluß in einer Datei enthalten ist.

2 Gehen Sie zum Abschnitt ‘Verzeichnis verschlüsseln – Standard’ auf Seite 48, Schritt 2. Folgen Sie diesem Vorgang, bis Sie angewiesen werden, hierher zurückzukehren.

3 Klicken Sie auf **Verschlüsseln**.

Ergebnis Privacy verschlüsselt das Verzeichnis und legt alle Unterverzeichnisse in einer verschlüsselten ausführbaren Datei namens *ihrverzeichnisname.Encrypted.exe* ab. Zum Beispiel *Geheimedateien.Encrypted.exe*

Datenträger verschlüsseln – Standard

➪ Eine Übersicht über die Verschlüsselung von Datenträgern finden Sie unter ‘Daten auf Datenträgern schützen’ auf Seite 5.

Hinweis Folgendes können Sie mit Privacy nicht verschlüsseln:

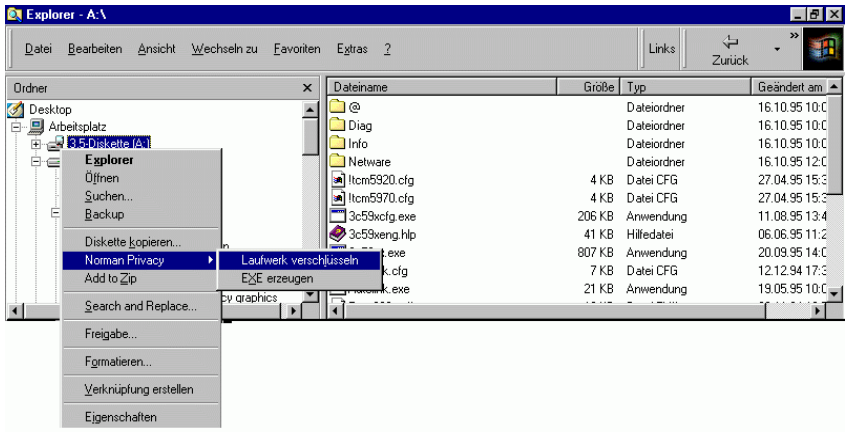
- die Systembereiche eines Datenträgers,
- entfernte (Netzwerk-) Laufwerke oder
- das Boot-Laufwerk (meist das Laufwerk C:, unter Umständen auch eine Diskette).

➪ Wenn Sie die oben genannten Elemente verschlüsseln möchten, verwenden Sie Norman Access Control für Windows 95/98, oder NT.

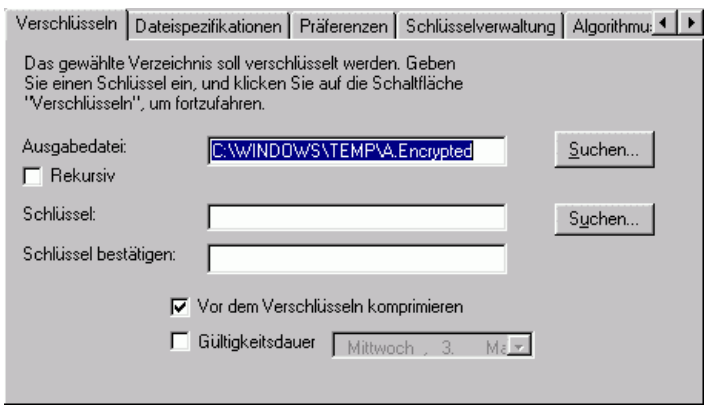
1 Klicken Sie im Windows Explorer mit der rechten Maustaste auf den Datenträger, den Sie verschlüsseln möchten, klicken Sie auf

Copyright © 2000 Norman

Norman Privacy und anschließend auf **Laufwerk verschlüsseln** (siehe unten).



Ergebnis Das folgende Dialogfeld wird angezeigt:



Hinweis Dieses Dialogfeld enthält das „ausgewählte Verzeichnis“, da das Hauptverzeichnis des Datenträgers verschlüsselt wird. Eine „Ausgabedatei“ wird erwähnt, weil der Inhalt des Datenträgers zum Schluß in einer Datei enthalten ist.

2 Behalten Sie entweder den Standardnamen für die Ausgabedatei bei, geben Sie einen neuen Namen in das Feld **Ausgabedatei** ein, oder klicken Sie auf **Suchen**, und wählen Sie einen Dateinamen aus.

Hinweis Wenn Sie Informationen verschlüsseln möchten, die ***30 % oder weniger*** des Datenträgerplatzes in Anspruch nehmen (oder bis zu 50 %, wenn Sie die verschlüsselten Informationen komprimieren möchten), und Sie die verschlüsselten

Copyright © 2000 Norman

Informationen auf demselben Datenträger speichern möchten, geben Sie der Ausgabedatei den Namen *A:\A.Encrypted*. Wenn Sie Informationen verschlüsseln möchten, die ***mehr als 30 %*** des Datenträgerplatzes in Anspruch nehmen (oder über 50 %, wenn Sie die verschlüsselten Informationen komprimieren möchten), und Sie die verschlüsselten Informationen auf demselben Datenträger speichern möchten, ist die schnellste Möglichkeit, die Dateien unter *C:\Windows\Temp\A.Encrypted* zu verschlüsseln und die verschlüsselten Dateien auf den Datenträger zu kopieren.

3 Wenn Sie alle Daten in allen Verzeichnissen des Datenträgers verschlüsseln möchten, klicken Sie auf **Rekursiv**.

4 Geben Sie einen Schlüssel ein, oder klicken Sie auf **Suchen** neben dem Feld **Schlüssel**, und doppelklicken Sie auf einen Aliasnamen im Dialogfeld **Schlüsselwahl**.

Hinweis Geben Sie keinen Aliasnamen in das Feld **Schlüssel** ein. Wenn Sie den Schlüssel eines Aliasnamens verwenden möchten, müssen Sie den Aliasnamen im Dialogfeld **Schlüsselwahl** auswählen.

Ergebnis Privacy zeigt Sternchen (*) im Dialogfeld **Schlüssel** an.

5 Wenn Sie das Verzeichnis ***nicht*** komprimieren möchten, deaktivieren Sie die Option **Vor dem Verschlüsseln komprimieren**.

6 Wenn Sie ***kein*** Ablaufdatum festlegen möchten, zu dem der verschlüsselte Text nicht mehr zugänglich ist, ***fahren Sie mit*** Schritt 8 ***fort***.

Wenn Sie ein Ablaufdatum festlegen ***möchten***, klicken Sie auf **Gültigkeitsdauer** und dann auf den Pfeil neben dem Datum.

Ergebnis Das folgende Dialogfeld erscheint mit dem aktuellen Datum eingekreist:

Copyright © 2000 Norman

7 Klicken Sie auf das Datum, zu dem die Datei ablaufen soll. Wenn Sie ein Datum im Feld **Gültigkeitsdauer** ändern möchten, klicken Sie auf den entsprechenden Tag, Monat oder das Jahr, und verwenden Sie die Pfeiltasten.

Ergebnis Das Dialogfeld **Verschlüsseln** wird erneut angezeigt.

8 Legen Sie fest, wie die Originaldatei verarbeitet werden soll.

➪ 'Originaldateien' auf Seite 34.

9 Legen Sie gegebenenfalls zusätzliche Sicherheits- und Informationseinstellungen fest.

➪ 'Zusätzliche Sicherheitseinstellungen' auf Seite 36.

10 Haben Sie diesen Vorgang ausgehend vom Abschnitt 'Datenträger verschlüsseln – selbstentschlüsselnd' auf Seite 55 gelesen?

11 ***Ja*** Fahren Sie mit Schritt 3 in diesem Vorgang fort.
Nein Fahren Sie mit Schritt 11 fort.

12 Klicken Sie auf **Verschlüsseln**.

Ergebnis Privacy verschlüsselt den Datenträger und zeigt anschließend das Explorer-Fenster mit dem Inhalt des verschlüsselten Datenträgers an.
Der verschlüsselte Datenträger enthält die verschlüsselten Versionen aller Daten auf diesem Datenträger.

Datenträger verschlüsseln – selbstentschlüsselnd

➪ Eine Übersicht über die Verschlüsselung von Datenträgern finden Sie unter 'Daten auf Datenträgern schützen' auf Seite 5.

Hinweis Folgendes können Sie mit Privacy nicht verschlüsseln

- die Systembereiche eines Datenträgers,
- entfernte (Netzwerk-) Laufwerke oder
- das Boot-Laufwerk (meist das Laufwerk C:, unter Umständen auch eine Diskette).

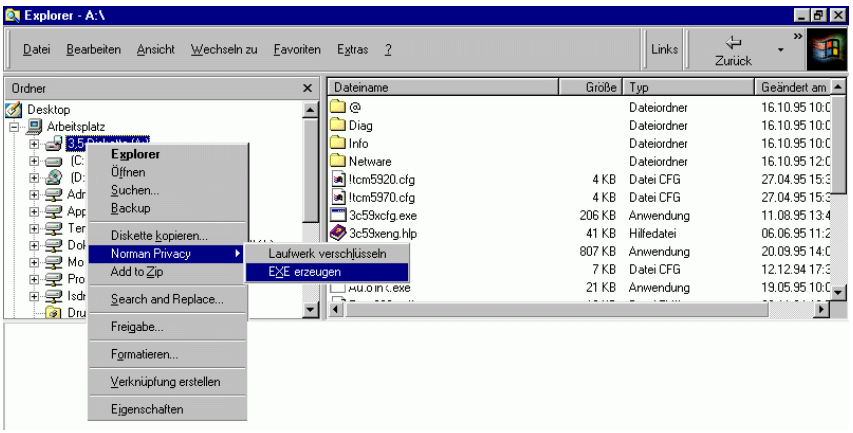
➪ Wenn Sie die oben genannten Elemente verschlüsseln möchten, verwenden Sie Norman Access Control für Windows 95/98, oder NT.

Hinweis Wenn der Datenträger bereits verschlüsselt ist, wird er im Explorer als eine verschlüsselte ***Datei*** angezeigt.

Copyright © 2000 Norman

➪ ‘Datei verschlüsseln – selbstentschlüsselnd’ auf Seite 47.

1 Klicken Sie im Windows Explorer mit der rechten Maustaste auf den Datenträger, für den Sie einen selbstentschlüsselnden Datenträger erstellen möchten, klicken Sie auf **Norman Privacy** und anschließend auf **EXE erzeugen**.



Ergebnis Das Privacy-Verschlüsselungsdialogfeld wird mit dem ausgewählten Datenträgernamen und der Erweiterung *Encrypted* angezeigt.

Hinweis Dieses Dialogfeld enthält eine „Ausgabedatei“, da der Inhalt des Datenträgers zum Schluß in einer Datei enthalten ist.

2 Gehen Sie zu ‘Datenträger verschlüsseln – Standard’ auf Seite 52, Schritt 2. Folgen Sie dem Vorgang, bis Sie angewiesen werden, hierher zurückzukehren.

3 Klicken Sie auf **Verschlüsseln**.

Ergebnis Privacy verschlüsselt den Datenträger und legt alle Verzeichnisse, Unterverzeichnisse und Dateien in einer verschlüsselten ausführbaren ***Datei*** namens *ihrdatenträgername.Encrypted.exe* ab.
Zum Beispiel *A:\A.Encrypted.exe*.

Copyright © 2000 Norman

Entschlüsseln

Dialogfeld Schlüsselwahl

Wenn Sie Informationen verschlüsseln, tun Sie dies, indem Sie einen Schlüssel eingeben oder einen Aliasnamen auswählen, für den Privacy dann den zugehörigen Schlüssel einfügt. In Privacy können Sie den gewünschten Aliasnamen auswählen.

1 Klicken Sie dazu in einem beliebigen Privacy-Verschlüsselungsdialogfeld auf **Suchen** neben dem Feld **Schlüssel**.

Ergebnis Das Dialogfeld **Schlüsselwahl** wird mit Ihren Benutzerprofilen und Aliasnamen angezeigt.

2 Doppelklicken Sie auf den Aliasnamen, dessen Schlüssel Sie aufrufen möchten.

Ergebnis Privacy fügt den Schlüssel in das Feld **Schlüssel** ein.

Copyright © 2000 Norman

Eine vollständige E-Mail mit oder ohne Anhänge entschlüsseln

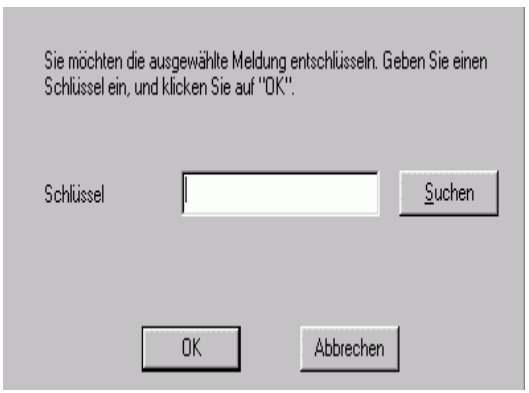
➪ Eine Übersicht über die Verschlüsselung von E-Mails finden Sie unter ‘E-Mails verschlüsseln und entschlüsseln’ auf Seite 8.

1 Zeigt Ihr E-Mail-Programm die Symbole und in der Symbolleiste an?

Ja Fahren Sie mit Schritt 2 fort.

Nein Informationen zum Entschlüsseln des ***Nachrichtentexts*** finden Sie unter ‘Text entschlüsseln’ auf Seite 60.
Informationen zum Entschlüsseln des ***Anhangs*** finden Sie unter ‘Datei entschlüsseln – Standard’ auf Seite 61 oder ‘Selbstentschlüsselnde Datei, Verzeichnis oder Datenträger entschlüsseln’ auf Seite 63.

2 Wenn Sie eine verschlüsselte E-Mail in Ihrem Postfach öffnen, wird folgendes Dialogfeld angezeigt:


Sie möchten die ausgewählte Meldung entschlüsseln. Geben Sie einen Schlüssel ein, und klicken Sie auf "OK".
Schlüssel
Suchen
OK
Abbrechen

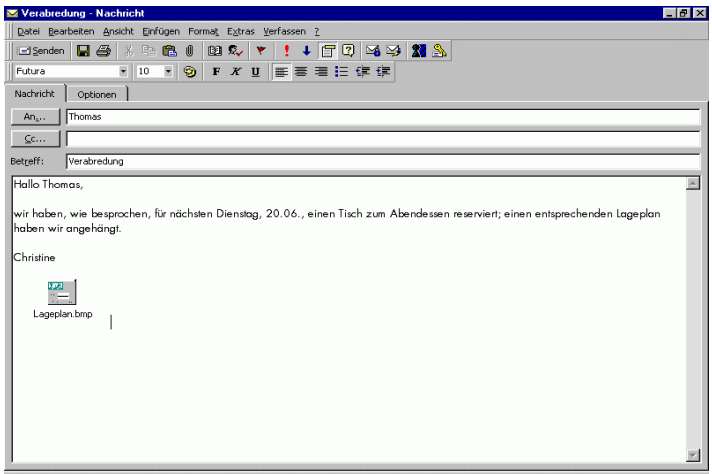
3 Geben Sie einen Schlüssel ein, oder klicken Sie auf **Suchen**, und wählen Sie im Dialogfeld **Schlüsselwahl** einen Aliasnamen aus.

Ergebnis Privacy zeigt Sternchen (*) im Feld **Schlüssel** an.

Copyright © 2000 Norman

4 Klicken Sie auf **OK**.

Ergebnis Privacy entschlüsselt den E-Mail-Nachrichtentext und zeigt die E-Mail in lesbarem Text an. Anhänge werden jetzt ***noch nicht*** entschlüsselt.



5 Wenn Sie den Anhang entschlüsseln möchten, doppelklicken Sie darauf.

Ergebnis Das Privacy-Entschlüsselungsdialogfeld wird geöffnet.

6 Behalten Sie entweder den Standard-Dateinamen bei, geben Sie einen neuen Dateinamen in das Feld **Ausgabedatei** ein, oder klicken Sie auf **Suchen**, und wählen Sie einen Dateinamen aus.

7 Geben Sie einen Schlüssel ein, oder klicken Sie auf **Suchen** neben dem Feld **Schlüssel** und doppelklicken Sie im Dialogfeld **Schlüsselwahl** auf einen Aliasnamen.

Ergebnis Privacy zeigt Sternchen (*) im Feld **Schlüssel** an.

8 Klicken Sie auf **Entschlüsseln**.

Ergebnis Privacy entschlüsselt die Datei.

Hinweis Wenn das Feld **Schlüssel** einen falschen Schlüssel enthält, zeigt Privacy eine Meldung an, die besagt, daß sich der eingegebene Schlüssel von dem Schlüssel unterscheidet, der zur Verschlüsselung eingegeben wurde. Klicken Sie auf **OK**, und geben Sie den richtigen Schlüssel ein.

Copyright © 2000 Norman

Text entschlüsseln

➪ ‘Text schützen’ auf Seite 7.

Folgen Sie diesen Schritten, um Text in einer beliebigen Anwendung zu entschlüsseln, die den Einsatz der Zwischenablage unterstützt.

1 Wählen Sie den Text aus, den Sie entschlüsseln möchten. Stellen Sie dabei sicher, daß Sie den vollständigen Platzhalter-Text markieren:
„*** Start Norman Privacy Privacy ***“
und
„*** Stop Norman Privacy Privacy ***“.

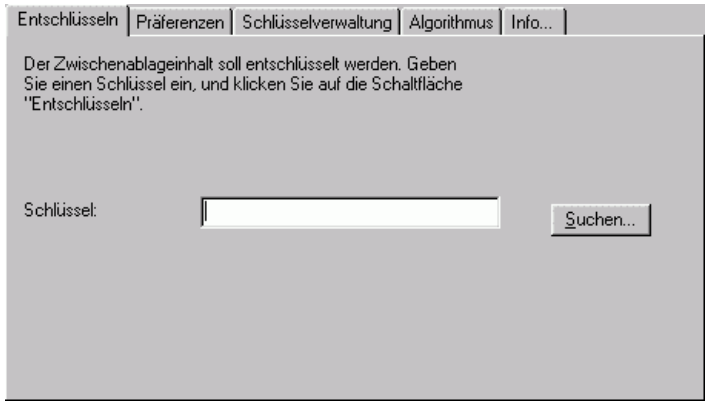
Hinweis Stellen Sie sicher, daß beide Zeilen des Platzhalter-Texts eine gesamte Zeile einnehmen. Wenn das Fenster so schmal ist, daß der Text auf eine zweite Zeile umbricht, kann Privacy den Text möglicherweise nicht problemlos entschlüsseln.

2 Kopieren Sie Ihre Auswahl in die Zwischenablage. Drücken Sie dazu zum Beispiel **Strg + C**.

3 Klicken Sie auf das Zwischenablage-Symbol in der Task-Leiste und anschließend auf **Zwischenablage entschlüsseln**.

Ergebnis Das folgende Dialogfeld erscheint:

Copyright © 2000 Norman



4 Geben Sie einen Schlüssel ein, oder klicken Sie auf **Suchen** neben dem Feld **Schlüssel** und doppelklicken Sie im Dialogfeld **Schlüsselwahl** auf einen Aliasnamen.

Ergebnis Privacy zeigt Sternchen (*) im Feld **Schlüssel** an.

5 Klicken Sie auf **Entschlüsseln**.

Ergebnis Privacy entschlüsselt den Text und legt ihn in der Zwischenablage ab.

Hinweis Wenn das Feld **Schlüssel** einen falschen Schlüssel enthält, zeigt Privacy eine Meldung an, die besagt, daß sich der eingegebene Schlüssel von dem Schlüssel unterscheidet, der zur Verschlüsselung eingegeben wurde. Klicken Sie auf **OK**, und geben Sie den richtigen Schlüssel ein.

6 Fügen Sie den Text aus der Zwischenablage über dem verschlüsselten Text ein. Drücken Sie dazu beispielsweise **Strg + V**.

Ergebnis Der entschlüsselte Text ersetzt den verschlüsselten Text.

Datei entschlüsseln – Standard

➪ Eine Übersicht über die Entschlüsselung von Dateien finden Sie unter ‘Informationen in Dateien schützen’ auf Seite 6.

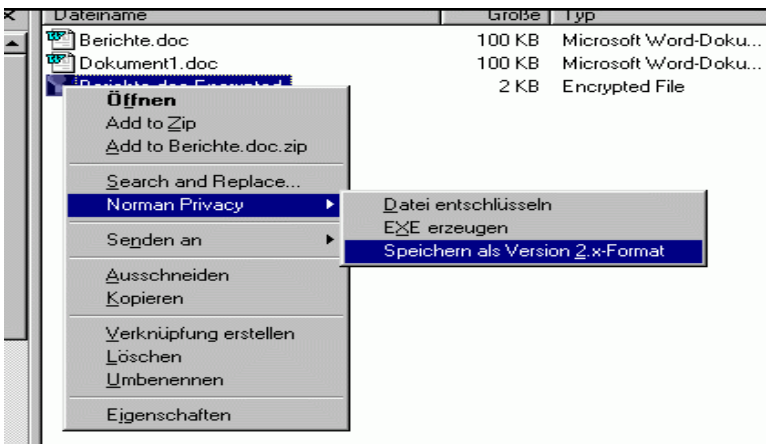
1 Gehen Sie im Windows Explorer oder in einem seiner Dialogfelder (Speichern, Speichern unter, Öffnen oder Suchen) folgendermaßen vor:

Copyright © 2000 Norman

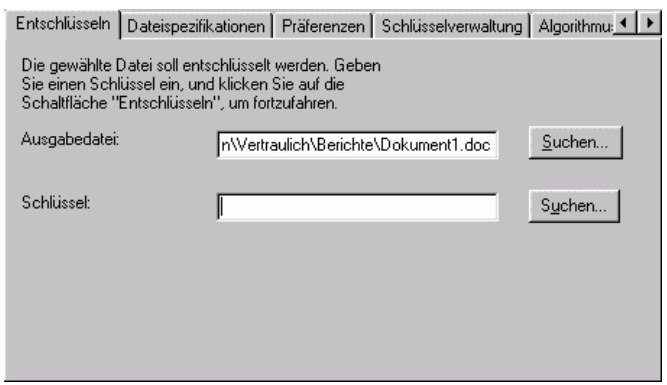
- ziehen Sie die Datei auf das Desktop-Symbol für **Privacy**

, ***oder***

- doppelklicken Sie auf die verschlüsselte Datei, ***oder***
- klicken Sie mit der rechten Maustaste auf die Datei, die Sie entschlüsseln möchten, klicken Sie auf Norman **Privacy** und anschließend auf **Datei entschlüsseln** (siehe unten).



Ergebnis Das folgende Dialogfeld wird geöffnet und der ausgewählte Dateiname wird ***ohne den Status „Verschlüsselt“*** im Feld **Ausgabedatei** angezeigt.



Hinweis Wenn Sie sich entscheiden, daß Sie eine andere Datei verschlüsseln möchten, ziehen Sie die Datei einfach aus dem Windows Explorer, und legen Sie sie auf dem Privacy-

Copyright © 2000 Norman

Dialogfeld ab. Der Name der **Ausgabedatei** ändert sich automatisch.

2 Behalten Sie entweder den Standard-Dateinamen bei, geben Sie einen neuen Dateinamen in das Feld **Ausgabedatei** ein, oder klicken Sie auf **Suchen**, und wählen Sie einen Dateinamen aus.

3 Geben Sie einen Schlüssel ein, oder klicken Sie auf **Suchen** neben dem Feld **Schlüssel** und doppelklicken Sie im Dialogfeld **Schlüsselwahl** auf einen Aliasnamen.

Ergebnis Privacy zeigt Sternchen (*) im Feld **Schlüssel** an.

4 Klicken Sie auf **Entschlüsseln**.

Ergebnis Privacy entschlüsselt die Datei.

Hinweis Wenn das Feld **Schlüssel** einen falschen Schlüssel enthält, zeigt Privacy eine Meldung an, die besagt, daß sich der eingegebene Schlüssel von dem Schlüssel unterscheidet, der zur Verschlüsselung eingegeben wurde. Klicken Sie auf **OK**, und geben Sie den richtigen Schlüssel ein.

Selbstentschlüsselnde Datei, Verzeichnis oder Datenträger entschlüsseln

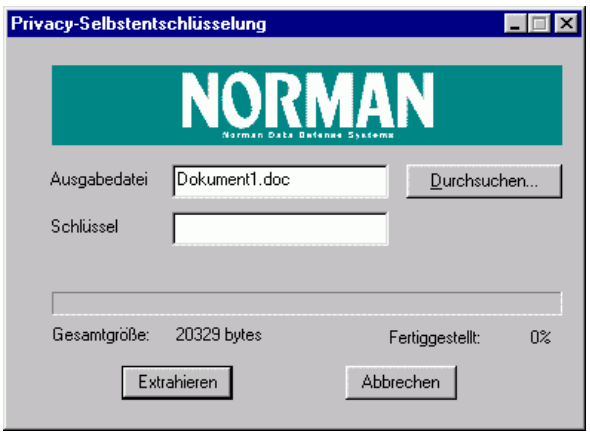
➪ Informationen zur Selbstentschlüsselung finden Sie unter ‘Selbstentschlüsselnde Dateien, Verzeichnisse und Datenträger’ auf Seite 8.

1 Doppelklicken Sie im Windows Explorer oder einem seiner Dialogfelder (Speichern, Speichern unter, Öffnen oder Suchen) auf die Datei *ihrdateiname.Encrypted.exe*, *ihrverzeichnisname.Encrypted.exe* oder *ihrdatenträgername.Encrypted.exe*.

Ergebnis Das folgende Dialogfeld wird mit dem Namen der verschlüsselten Datei, des verschlüsselten Verzeichnisses oder

Copyright © 2000 Norman

Datenträgers angezeigt, die Sie ***ohne den Status .Encrypted*** im Feld **Ausgabedatei** ausgewählt haben:



2 Geben Sie den Schlüssel oder Aliasnamen ein, der zum Verschlüsseln der Datei, des Verzeichnisses oder Datenträgers verwendet wurde, und klicken Sie auf **Extrahieren**.

Ergebnis Die Datei wird entschlüsselt. Privacy zeigt eine Meldung an, die besagt, daß der Vorgang erfolgreich ausgeführt wurde.

Hinweis Wenn das Feld **Schlüssel** einen falschen Schlüssel enthält, zeigt Privacy eine Meldung an, die besagt, daß sich der eingegebene Schlüssel von dem Schlüssel unterscheidet, der zur Verschlüsselung eingegeben wurde. Klicken Sie auf **OK**, und geben Sie den richtigen Schlüssel ein.

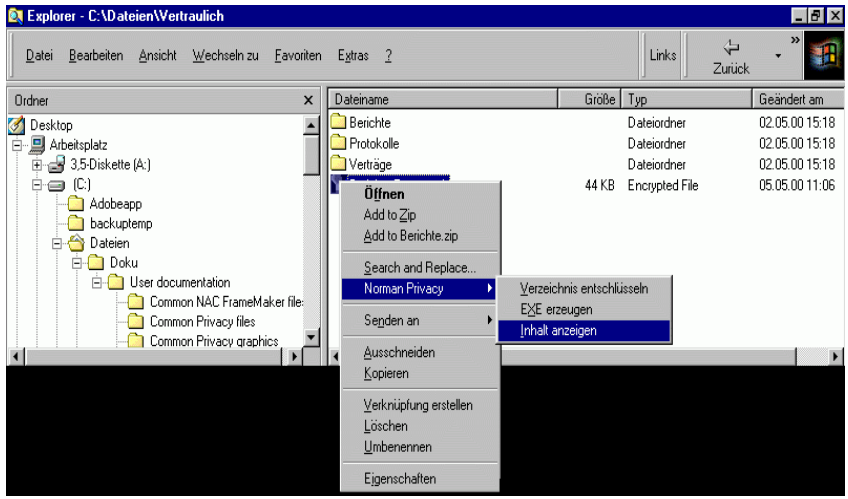
Inhalt eines verschlüsselten Verzeichnisses anzeigen

Hinweis Ein verschlüsseltes Verzeichnis wird im Explorer als eine Datei *ihrverzeichnisname.Encrypted* angezeigt.

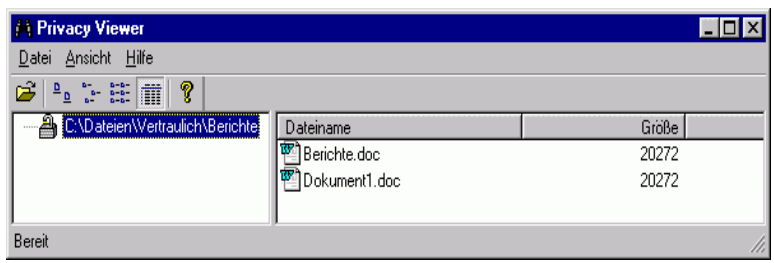
1 Klicken Sie im Windows Explorer oder in einem seiner Dialogfelder (Speichern, Speichern unter, Öffnen oder Suchen) mit der rechten Maustaste auf das verschlüsselte Verzeichnis, dessen Inhalt Sie

Copyright © 2000 Norman

anzeigen möchten, klicken Sie auf **Norman Privacy** und dann auf **Inhalt anzeigen**.



Ergebnis Das folgende Dialogfeld erscheint:



2 Klicken Sie auf die Verzeichnisse, um deren Inhalt anzuzeigen.

3 Wenn Sie ***einzelne Dateien*** in dem verschlüsselten Verzeichnis anzeigen möchten, lesen Sie den Abschnitt ‘Einzelne Dateien aus einem verschlüsselten Datenträger oder Verzeichnis entschlüsseln’ auf Seite 66.
Möchten Sie das ***gesamte Verzeichnis*** entschlüsseln, lesen Sie den Abschnitt ‘Verzeichnis entschlüsseln – Standard’ auf Seite 68.

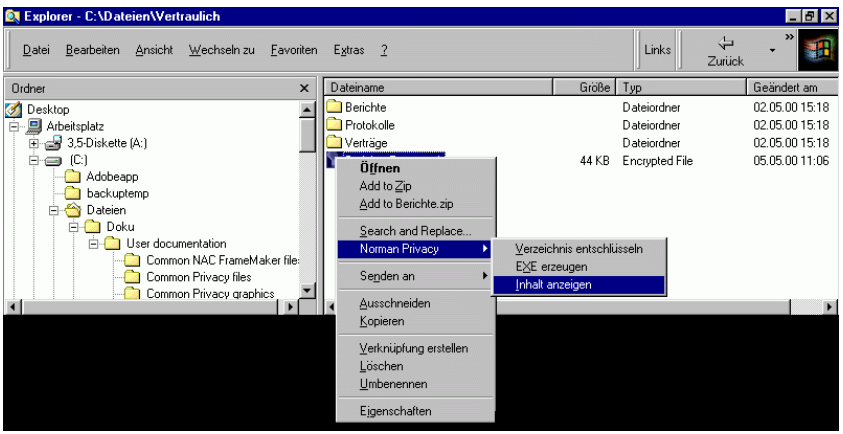
Copyright © 2000 Norman

Einzelne Dateien aus einem verschlüsselten Datenträger oder Verzeichnis entschlüsseln

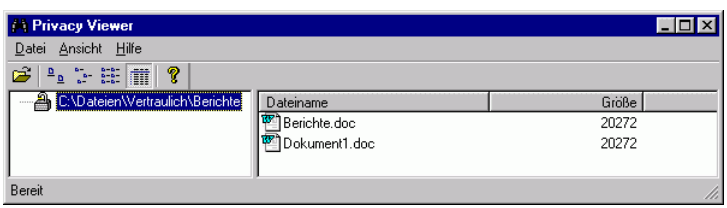
Gehen Sie folgendermaßen vor, um mit dem Privacy Viewer eine oder mehrere Dateien aus einem verschlüsselten Datenträger oder Verzeichnis zu entschlüsseln.

Hinweis Ein verschlüsseltes Verzeichnis erscheint im Explorer unter dem Dateinamen *ihrverzeichnisname.Encrypted*.

1 Klicken Sie im Windows Explorer oder in einem seiner Dialogfelder (Speichern, Speichern unter, Öffnen oder Suchen) mit der rechten Maustaste auf den verschlüsselten Datenträger oder das verschlüsselte Verzeichnis mit den Verzeichnissen oder Dateien, die Sie entschlüsseln möchten, klicken Sie auf **Norman Privacy** und dann auf **Inhalt anzeigen**.



Ergebnis Das folgende Dialogfeld wird angezeigt:



2 Klicken Sie mit der rechten Maustaste auf den Namen der Datei, die Sie entschlüsseln möchten, und klicken Sie auf **Entschlüsseln**.

Copyright © 2000 Norman

Hinweis Wenn Sie mehrere Dateien auf einmal entschlüsseln möchten, halten Sie die Taste **Strg** gedrückt, und klicken Sie auf die verschiedenen Dateien.

Ergebnis Folgendes Dialogfeld wird angezeigt:

3 Behalten Sie entweder die Standardposition für die extrahierte Datei oder das extrahierte Verzeichnis bei, geben Sie eine neue Position in das Feld **Extrahieren nach** ein, oder klicken Sie auf **Suchen**, und wählen Sie eine Position aus.

4 Geben Sie einen Schlüssel in das Feld **Schlüssel** ein, oder klicken Sie auf **Suchen**, und doppelklicken Sie im Dialogfeld **Schlüsselwahl** auf den gewünschten Aliasnamen.

Hinweis Wenn die Schaltfläche **Suchen** nicht verfügbar ist, sind Sie nicht bei Privacy angemeldet. Schließen Sie den Privacy Viewer, melden Sie sich bei Privacy an, und öffnen Sie den Viewer erneut.

Ergebnis Privacy zeigt Sternchen (*) im Feld **Schlüssel** an.

5 Klicken Sie auf **OK**.

Ergebnis Privacy entschlüsselt die Datei.

Hinweis Wenn das Feld **Schlüssel** einen falschen Schlüssel enthält, zeigt Privacy eine Meldung an, die besagt, daß sich der eingegebene Schlüssel von dem Schlüssel unterscheidet, der zur Verschlüsselung eingegeben wurde. Klicken Sie auf **OK**, und geben Sie den richtigen Schlüssel ein.

Copyright © 2000 Norman

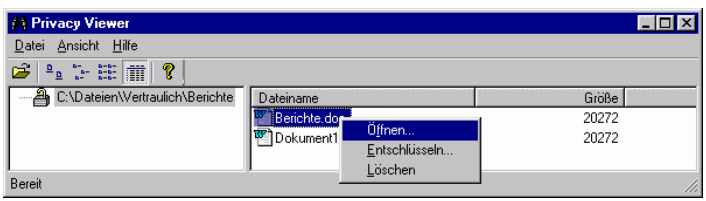
Verschlüsselte Datei im Privacy Viewer entschlüsseln und öffnen

Verwenden Sie diese Vorgehensweise, um eine Datei in ihrer jeweiligen Anwendung zu entschlüsseln und zu öffnen.

1 Zeigen Sie die Datei im Privacy Viewer an.

➪ ‘Inhalt eines verschlüsselten Verzeichnisses anzeigen’ auf Seite 64.

2 Doppelklicken Sie auf die Datei, die Sie öffnen möchten, oder klicken Sie mit der rechten Maustaste auf die Datei, und klicken Sie auf **Öffnen**.



3 Geben Sie einen Schlüssel in das Feld **Schlüssel** ein, oder klicken Sie auf **Suchen**, und doppelklicken Sie im Dialogfeld **Schlüsselwahl** auf den gewünschten Aliasnamen.

Ergebnis Privacy zeigt Sternchen (*) im Feld **Schlüssel** an.

4 Klicken Sie auf **OK**.

Ergebnis Die mit der Datei verknüpfte Anwendung wird geöffnet, dann wird die Datei geöffnet.

Verzeichnis entschlüsseln – Standard

Gehen Sie folgendermaßen vor, um den Inhalt eines gesamten Verzeichnisses auf einmal zu entschlüsseln.

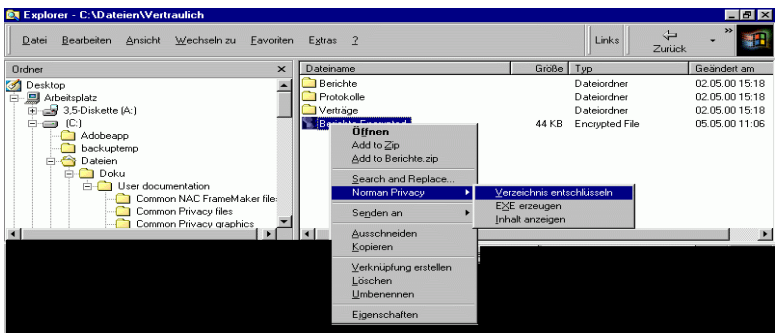
➪ Eine Übersicht über die Verschlüsselung von Verzeichnissen finden Sie unter ‘Informationen in Verzeichnissen schützen’ auf Seite 6.

Hinweis Ein verschlüsseltes Verzeichnis erscheint im Explorer unter dem Dateinamen *ihrverzeichnisname.Encrypted*.

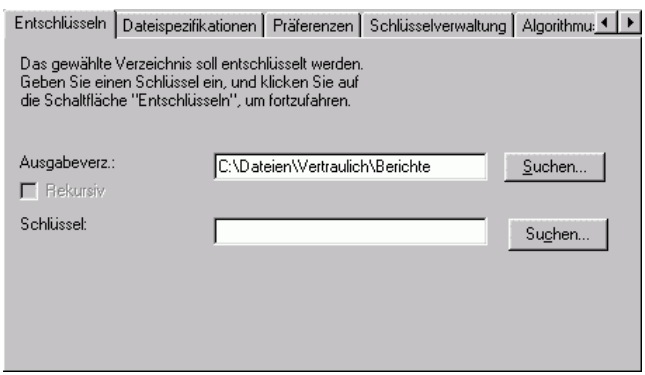
1 Gehen Sie im Windows Explorer oder in einem seiner Dialogfelder (Speichern, Speichern unter, Öffnen oder Suchen) folgendermaßen vor:

Copyright © 2000 Norman

- ziehen Sie das verschlüsselte Verzeichnis auf das Desktop-Symbol für **Privacy** , ***oder***
- doppelklicken Sie auf das verschlüsselte Verzeichnis, ***oder***
- klicken Sie mit der rechten Maustaste auf das Verzeichnis, das Sie entschlüsseln möchten, klicken Sie auf **Norman Privacy** und anschließend auf **Verzeichnis entschlüsseln** (siehe unten).



Ergebnis Das folgende Dialogfeld wird angezeigt und der ausgewählte Verzeichnisname wird ***ohne den Status „Encrypted“*** im Feld **Ausgabeverzeichnis** angezeigt.



Hinweis Wenn Sie sich entscheiden, daß Sie eine andere Datei entschlüsseln möchten, ziehen Sie die Datei einfach aus dem Windows Explorer, und legen Sie sie auf dem Privacy-Dialogfeld ab. Der Name der **Ausgabedatei** ändert sich automatisch.

Copyright © 2000 Norman

2 Behalten Sie entweder den Standard-Verzeichnisnamen bei, geben Sie einen neuen Verzeichnisnamen in das Feld **Ausgabeverzeichnis** ein, oder klicken Sie auf **Suchen**, und wählen Sie einen Verzeichnisnamen aus.

Hinweis Wenn Sie die Daten in allen Verzeichnissen des verschlüsselten Datenträgers verschlüsselt haben, entschlüsselt Privacy automatisch rekursiv alle.

3 Geben Sie einen Schlüssel in das Feld **Schlüssel** ein, oder klicken Sie auf **Suchen**, und doppelklicken Sie im Dialogfeld **Schlüsselwahl** auf den gewünschten Aliasnamen.

Ergebnis Privacy zeigt Sternchen (*) im Feld **Schlüssel** an.

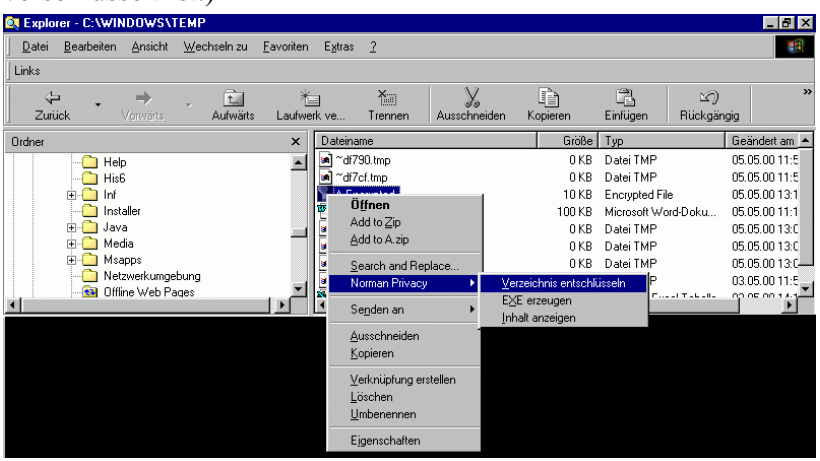
4 Klicken Sie auf **Entschlüsseln**.

Ergebnis Privacy entschlüsselt das Verzeichnis.

Hinweis Wenn das Feld **Schlüssel** einen falschen Schlüssel enthält, zeigt Privacy eine Meldung an, die besagt, daß sich der eingegebene Schlüssel von dem Schlüssel unterscheidet, der zur Verschlüsselung eingegeben wurde. Klicken Sie auf **OK**, und geben Sie den richtigen Schlüssel ein.

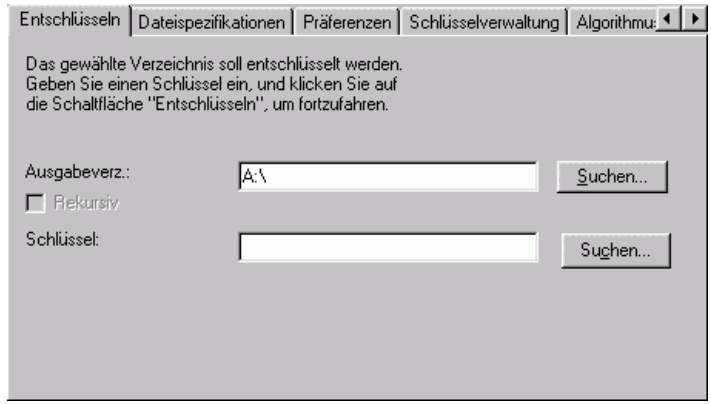
Datenträger entschlüsseln – Standard

1 Klicken Sie mit der rechten Maustaste auf den Datenträger, den Sie entschlüsseln möchten, klicken Sie auf **Norman Privacy** und dann auf **Verzeichnis entschlüsseln**. (Es lautet „Verzeichnis“, weil in der verschlüsselten Datei das Hauptverzeichnis des Datenträgers verschlüsselt ist.)



Copyright © 2000 Norman

Ergebnis Das folgende Dialogfeld erscheint:



2 Behalten Sie entweder den Standard-Verzeichnisnamen bei, geben Sie einen neuen Verzeichnisnamen in das Feld **Ausgabeverzeichnis** ein, oder klicken Sie auf **Suchen**, und wählen Sie einen Verzeichnisnamen aus.

3 Geben Sie einen Schlüssel in das Feld **Schlüssel** ein, oder klicken Sie auf **Suchen**, und doppelklicken Sie im Dialogfeld **Schlüsselwahl** auf den gewünschten Aliasnamen.

Ergebnis Privacy zeigt Sternchen (*) im Dialogfeld **Schlüssel** an.

4 Klicken Sie auf **Entschlüsseln**.

Ergebnis Privacy entschlüsselt das Hauptverzeichnis.

Hinweis Wenn das Feld **Schlüssel** einen falschen Schlüssel enthält, zeigt Privacy eine Meldung an, die besagt, daß sich der eingegebene Schlüssel von dem Schlüssel unterscheidet, der zur Verschlüsselung eingegeben wurde. Klicken Sie auf **OK**, und geben Sie den richtigen Schlüssel ein.

Copyright © 2000 Norman

Häufige Fragen

Frage	Lösung
Wie lautet die Standard-Benutzerkennung und das Standardkennwort?	**Benutzerkennung**Admin **Kennwort** admin
Wie lang darf meine Anmelde-Benutzerkennung sein?	Zwischen 1 und 255 Zeichen.
Wie lang darf mein Anmeldekennwort sein?	Zwischen 1 und 56 Zeichen.
Wie lang darf ein Benutzerprofilname sein?	Zwischen 1 und 255 Zeichen.
Wie lang darf ein Aliasname sein?	Zwischen 1 und 255 Zeichen.
Wie viele Aliasnamen/Schlüssel darf ich erstellen?	So viele, wie der Festplattenspeicher zuläßt!
Wie lang darf ein Schlüssel sein?	Zwischen 1 und 56 Zeichen.
Warum kann ich mein verschlüsseltes Verzeichnis nach der Verschlüsselung nicht wiederfinden?	Privacy speichert ein verschlüsseltes Verzeichnis in demselben Verzeichnis, in dem sich auch das Originalverzeichnis befindet. Wenn Sie zum Beispiel das Verzeichnis *C:\Meinedokumente\Berichte* verschlüsseln, speichert Privacy das entstehende verschlüsselte Verzeichnis unter *C:\Meinedokumente\Berichte.Encrypted*.

Copyright © 2000 Norman

Frage	Lösung
Warum verschwindet die Originaldatei bzw. das Originalverzeichnis nach der Verschlüsselung?	Die Option **Löschen der Originaldateien und -verzeichnisse** ist ausgewählt. Wenn Sie Ihre Originaldateien beibehalten möchten, öffnen Sie das Dialogfeld **Dateispezifikationen**, und deaktivieren Sie diese Option.
Welche E-Mail-Anwendungen werden von Privacy unterstützt?	Zum Zeitpunkt der Veröffentlichung unterstützt Privacy die Vollversionen von Microsoft Exchange und Microsoft Outlook.
Wenn ich eine teilweise verfaßte E-Mail-Nachricht vor dem Senden speichere, wird sie dann verschlüsselt?	Wenn Sie auf die Schaltfläche **Verschlüsseln beim Senden** klicken, bevor Sie die Nachricht speichern, verschlüsselt Privacy die Meldung, wenn Sie sie speichern. Wenn Sie die Nachricht öffnen, fertigstellen und senden, fordert Privacy Sie vor dem Verschlüsseln und Senden zur erneuten Eingabe des Schlüssels auf.
Können Personen, die Privacy nicht installiert haben, meine verschlüsselten E-Mails entschlüsseln?	Nein. Sie können ihnen jedoch eine selbstentschlüsselnde Datei als Anlage senden. Diese können sie dann entschlüsseln und lesen.
Warum kann ich keine Festplatten verschlüsseln?	Privacy ist nicht für das Verschlüsseln von Festplatten oder Festplattenpartitionen ausgelegt.

Copyright © 2000 Norman

Frage	Lösung
Kann ich Privacy 3.0 zum Entschlüsseln von Informationen verwenden, die mit Privacy 2.x oder 1.x verschlüsselt wurden?	Ja.
Kann ich Privacy 2.x oder 1.x zum Entschlüsseln von Informationen verwenden, die mit Privacy 3.x verschlüsselt wurden?	Nein, speichern Sie die Datei mit Privacy 3.0 als Version 2.x, und lesen Sie sie dann mit Privacy 2.x.
Kann ich die Import- und Exportfunktionen von Privacy über alle Privacy-Versionen verwenden?	Ja.

Copyright © 2000 Norman

Fehlerbehebung

Problem	Lösung
Was kann ich tun, wenn ich mein Privacy-Anmeldekennwort vergessen habe?	Wenn Sie Ihr Anmeldekennwort vergessen haben, können Sie sich unter keinen Umständen bei Privacy anmelden und auf Ihre Profile, Aliasnamen und Kennwörter zugreifen. *Behalten Sie Ihr Kennwort also immer im Gedächtnis!* Wenn Sie Ihr Kennwort vergessen haben, müssen Sie sich **1** mit der Benutzerkennung **Admin** und einem neu erstellten Kennwort bei Privacy anmelden. *More* Unter 'Vorgehensweise bei der ersten Anmeldung – eine Checkliste' auf Seite 14 und 'Benutzerkennung hinzufügen' auf Seite 21 finden Sie die Empfehlung, ein anderes Anmeldekennwort zu erstellen. **2** Fügen Sie einen neuen Benutzer für sich selbst hinzu, und richten Sie Ihre Benutzerprofile, Aliasnamen und Schlüssel erneut ein. *More* 'Schlüssel erstellen' auf Seite 17.

Copyright © 2000 Norman

Problem	Lösung
Wenn ich eine verschlüsselte E-Mail verschicke, erhalte ich keine Bestätigungsmeldung.	Das ist in Ordnung. Wenn eine verschlüsselte E-Mail gesendet wird, erscheint eine Statusanzeige auf dem Bildschirm. Wird diese Anzeige ausgeblendet, wissen Sie, daß Ihre verschlüsselte Nachricht erfolgreich gesendet wurde.
Ich erhalte eine Zugriffsverletzungsmeldung.	Sie versuchen, Informationen zu verschlüsseln, die momentan in einer anderen Anwendung geöffnet sind. Schließen Sie die Datei in der anderen Anwendung, und verschlüsseln Sie die Informationen erneut.

Copyright © 2000 Norman

Index

—A—

Abkürzungen in diesem Handbuch 1
Ablaufdatum
  Beispiel für Verwendung 5
  Festlegen für
    Dateiverschlüsselung 46
    Datenträger-Verschlüsselung 54
    Verzeichnisverschlüsselung 50
Aktivieren von Algorithmen 39
Aktualisieren einer vorhandenen Datenbank 20
Algorithmen
  Auswählen für Privacy 39
  Beschreibung 9
  Eigene in Privacy verwenden 10
  Einsatz in Privacy 9
  Für Sicherheit in Privacy 10
  Installieren anderer in Privacy 39
  Sicherheitsunterschiede zwischen 10
  Welche Schlüssel verwendet werden können 10
aliases
  encrypted in database 19
  where stored 19
aliases, Privacy
  associated passwords encrypted 19
  security 19
Aliasnamen, Privacy 11, 27
  Ändern 32
  Auswählen zum Verschlüsseln/Entschlüsseln 40, 57
  Hinzufügen 31
  Informationen 18
  Löschen 33
  Max. Länge 19
  Mindestlänge 19
  Sicherheit 19
  Unterschied zur Verwendung von Schlüsseln 18
  Verschlüsselt von Privacy-Anmeldekennwort 19
  Verwenden zum Verschlüsseln/Entschlüsseln von Informationen 10
  Warum verwenden? 18
  Zusammengehörige gruppieren 19
Ändern
  Algorithmen in Privacy 39
  Aliasnamen in Privacy 32
  Benutzerkennungen in Privacy 23
  Benutzerprofilnamen 27
  Privacy-Anmeldekennwort 15
  Schlüssel 32
Anmelden
  Ändern des Privacy-Anmeldekennworts 15
  Bei vergessenem Anmeldekennwort 75
  Privacy 13
  Vorgehensweise nach 14
Anzeigen
  Privacy-Dialogfeld 15
  Schlüsselwahl, Dialogfeld 40, 57
Attribute 34
Auswählen der Algorithmen für Privacy 39

—B—

Beibehalten der Zeitstempel 34
Benutzer
  Ändern einer Benutzerkennung in Privacy 23
  Hinzufügen in Privacy 21
  In Privacy 21
  Löschen in Privacy 24
  Max. Länge für Anmeldekennwort in Privacy 21
  Max. Länge für Benutzerkennung in Privacy 21
  Mindestlänge für Anmeldeken-

Copyright © 2000 Norman

nwort in Privacy 21
Mindestlänge für Benutzerkennung in Privacy 21
Wer sie in Privacy hinzufügen und ändern darf 23
Benutzer in Privacy 21
Benutzerkennung
Max. Länge 21
Mindestlänge 21
Wann eigene erstellen 21
Wer Benutzerprofile und Aliasnamen jeweils ändern darf 23
Benutzerprofile 11
Ändern des Namens 27
Datenbank, schnell aktualisieren 20
Exportieren 27
Hinzufügen 25
Importieren 29
Informationen 19
Löschen 30
Bestätigen des Schlüssels nach der manuellen Eingabe 36
Bestätigungsmeldung nach Ver-/Entschlüsselung 37
Bilder
Entschlüsseln 61
Entschlüsseln, Info 5
Verschlüsseln 45
Verschlüsseln, Info 5
Verschlüsseln/entschlüsseln 6
Blowfish-Algorithmen 9
Boot-Laufwerk 52, 55

—D—

database
for aliases & passwords 19
security 19
Dateieinstellungen
Original-Zeitstempel beibehalten 34
Dateien
Ablaufdatum, festlegen 46
Entschlüsseln 6
Entschlüsseln aus dem Privacy Viewer 66
Entschlüsseln aus einem verschlüsselten Verzeichnis 7, 66
Entschlüsseln, Standard 61, 68
Komprimieren vor der Verschlüsselung 46
Komprimierung 4
Öffnen wenn verschlüsselt 7, 68
Selbstentschlüsselnd 8
Verarbeiten der Originale 34
Verschlüsseln 6
Verschlüsseln & entschlüsseln 7
Verschlüsseln, selbstentschlüsselnd 47
Verschlüsseln, Standard 45
Verschlüsselt, öffnen 7, 68
Wiederherstellen 34
Zwei Möglichkeiten zum Verschlüsseln 6
Dateispezifikationen 34
Festlegen in Privacy 35
Sicheres Löschen der Originaldateien und -verzeichnisse 34
Daten
siehe Informationen
Datenbank
Für Aliasnamen & Schlüssel in Privacy 19
Privacy.mdb 19
Schnell für Benutzerprofile aktualisieren 20
Datenträger
Ablaufdatum, festlegen 54
Entschlüsseln, Info 5
Entschlüsseln, selbstentschlüsselnd 63
Entschlüsseln, Standard 70
Inhalt nach der Verschlüsselung 55
Komprimerung 4

Copyright © 2000 Norman

Komprimieren vor der Verschlüsselung 54
Komprimierung 4
Selbstentschlüsselnd 8
Systembereiche 5
Verschlüsseln, Info 5
Verschlüsseln, selbstentschlüsselnd 55
Verschlüsseln, Standard 52
Verschlüsselung des gesamten Datenträgers 5
Was Privacy nicht verschlüsselt 52, 55
Zwei Möglichkeiten zum Verschlüsseln 5
DES-Algorithmus 9
disk
see hard disks

—E—

Einrichten, Zusammenfassung 14
Einschränken des Zugriffs auf Schlüsselinformationen 21
Einschränken des Zugriffs auf Schlüsselverwaltung-Dialogfeld 36, 38
Einstellen
Voreinstellungen 37
Einstellungen, zusätzliche für Sicherheit 36
E-Mail 3
Entschlüsseln 7
Entschlüsseln von Text in 60
Entschlüsseln, mit oder ohne Anhänge 58
Verschlüsseln 7
Verschlüsseln von Text in 43
Verschlüsseln, mit oder ohne Anhänge 41
E-Mail-Adresse für Norman 2
Entfernte (Netzwerk-) Laufwerke 52, 55
Entschlüsseln
Dateien aus einem verschlüsselten Verzeichnis 66
Dateien, Standard 61, 68
Datenträger, selbstentschlüsselnd 63
Datenträger, Standard 70
E-Mail, vollständig, mit oder ohne Anhänge 58
Inhalt der Zwischenablage 60
Rekursive Verzeichnisse 70
Text 60
Wer darf 19
Entschlüsselung
Anzeigen einer Statusmeldung nach 37
Info 4
Modul 9
Was Sie entschlüsseln können 4
Wer es tun kann 4
Ziehen und Ablegen 69
Erstellt-Zeitstempel 34
Exportieren
Benutzerprofile 20, 27
Mehrere Aliasnamen 27
Mindestlänge für exportierten Schlüssel 29

—F—

Fehlerbehebung 75
Festlegen
Dateispezifikationen in Privacy 35
Festplattenspeicher, sparen 4

—G—

Geändert-Zeitstempel 34
Grafiken
Entschlüsseln 61
Entschlüsseln, Info 5
Verschlüsseln 45
Verschlüsseln, Info 5
Verschlüsseln/entschlüsseln 6

—H—

Häufige Fragen 72

Copyright © 2000 Norman

Hauptverzeichnis, verschlüsseln/entschlüsseln 5
Hinzufügen
  Aliasnamen in Privacy 31
  Benutzer in Privacy 21
  Profile 25
  Schlüssel 31

—I—

Importieren
  Benutzerprofile 20, 29
Info
  Algorithmen in Privacy 9
  Aliasnamen in Privacy 11, 18
  Benutzerprofile 11
  Dateispezifikationen 34
  Entschlüsselung 4
  Komprimeriung 4
  Originaldateien 34
  Schlüssel 11
  Verschlüsselung 4
  Zu diesem Handbuch 1
Informationen
  Benutzerprofile 19
  Benutzerprofile exportieren 20
  Benutzerprofile importieren 20
  Komprimierung 4
  Warum schützen? 3
Installieren
  Anderen Algorithmus in Privacy 39
  Privacy 12
Internet 3

—K—

Kennenlernen von Privacy 3
Komprimieren
  Dateien vor der Verschlüsselung 46
  Datenträger vor der Verschlüsselung 54
  Text vor der Verschlüsselung 44
  Verzeichnisse vor der Verschlüsselung 50
Komprimierung, Info 4
Konfigurieren
  Vor dem Konfigurieren von Privacy 3
  Zusätzliche Sicherheit für Verschlüsselung/Entschlüsselung 36
Konventionen in diesem Handbuch 1

—L—

logon password
  used to encrypt alias passwords 19
Löschen
  Aliasnamen in Privacy 33
  Benutzer in Privacy 24
  Benutzerprofile 30
  Schlüssel 33

—M—

Manuelle Eingabe eines Schlüssels 36

—N—

Norman Virus Control 12
Normans E-Mail-Adresse 2

—O—

Öffentliche Schlüssel 10
Ordner
  siehe Verzeichnisse
Originaldateien 34
  Sicher löschen nach Ver-/Entschlüsselung 34
  Verarbeiten 34
Originalverzeichnisse 34
  Sicher löschen nach Ver-/Entschlüsselung 34
  Verarbeiten 34

—P—

passwords
  encrypted by logon password 19

Copyright © 2000 Norman

encrypted in database 19
security 19
where stored 19
passwords, Privacy
encrypted by smartcard password 19
Privacy 3
Anmelden 13
database 19
Datenbank 19
Dialogfeld, anzeigen 15
Installieren 12
Kennenlernen 1
Verknüpfung zum Privacy-Dialogfeld 12
Was es ver- und entschlüsseln kann 4
Privacy Viewer
Anzeigen des Inhalts eines verschlüsselten Verzeichnisses 64
Entschlüsseln aus 66
Info 5, 6, 7
Öffnen verschlüsselter Dateien aus 68
Privacy.mdb, Datenbank 19
Privacy-Anmeldedialogfeld, wann es angezeigt wird 15
Privacy-Anmeldekennwort
Anmelden ohne 75
Anmelden wenn vergessen 75
Max. Länge 16, 21
Standard 3
Vergessen 75
Verwenden zum Einschränken des Zugriffs auf Schlüsselverwaltung-Dialogfeld 36
Verwendung zur Verschlüsselung von Aliasnamen und Schlüsseln in Privacy 19
Wann eigenes erstellen 21
Private Schlüssel 10
Profile
Importieren/Exportieren 20
Max. Länge 21
Mindestlänge 21
profiles
encrypted 20
encrypting database 20
how they are kept secure 20
where stored 20

—R—

Readme-Datei 12
Rekursive Verschlüsselung 6
Rekursive Verzeichnisse
Entschlüsseln 70
Verschlüsseln 49, 54

—S—

Schlüssel 11, 18
Siehe auch Schlüsselwahl, Dialogfeld
Ändern 32
Bestätigen nach der manuellen Eingabe 36
Eingabe im Gedächtnis behalten 36
Eingeben eines falschen beim Entschlüsseln 61, 70, 71
Einschränken des Zugriffs auf 21
Hinzufügen 31
Informationen 18
Löschen 33
Max. Länge 19
Mindestlänge 19
Mindestlänge für exportierten Schlüssel 29
Öffentlich 10
Privat 10
Sicherheit 19
Starke & weiche 18
Unterschied zur Verwendung eines Aliasnamens 18
Verschlüsselt von Privacy-Anmeldekennwort 19
Verschlüsselungssicherheit 10

Copyright © 2000 Norman

Verwenden zum Verschlüsseln/Entschlüsseln von Informationen 10
Warum verschiedene verwenden? 18
Wie anderen mitteilen 11
Wie viele erstellt werden können 11
Wozu Privacy sie verwendet 18
Schlüssel, Dialogfeld
Anzeigen 17
Schlüsselverwaltung-Dialogfeld
Einschränken des Zugriffs auf 36, 38
Schlüsselwahl, Dialogfeld 40, 57
Schützen
Dateien 6, 7
Datenträger 5
Text 7
Verzeichnisse 6
Selbstentschlüsselnd
Dateien 6
Dateien, erstellen 47
Datenträger 5
Datenträger, entschlüsseln 63
Datenträger, erstellen 55
Eigenschaft 8
Verzeichnisse 6
Verzeichnisse, entschlüsseln 63
Verzeichnisse, erstellen 51
Sicher löschen
Dateien nach Ver-/Entschlüsselung 34
Verzeichnisse nach Ver-/Entschlüsselung 34
Sicherer Zugriff auf Schlüsselverwaltung-Dialogfeld 38
Sicherheit
Unterschiede zwischen Algorithmen 10
Zusätzliche Sicherheitseinstellungen 36
smartcard password
used to encrypt alias passwords, Privacy 19
smartcards
password used to encrypt profiles 20
Sparen von Festplattenspeicher 4
Standard-Benutzerkennung und -Kennwort zum Anmelden bei Privacy
Standard 3
Standardverschlüsselung 7
Datei 6
Datenträger 5
Verzeichnis 6
Starke Schlüssel 18
Systembereiche eines Datenträgers 5, 52, 55

—T—

Text
Entschlüsseln 7, 60
Erscheinungsbild wenn verschlüsselt 44
Formatierung, Verlust nach Verschlüsselung 43
Komprimeriung 4
Komprimieren vor der Verschlüsselung 44
Max. Menge, die verschlüsselt werden kann 43
Verschlüsseln 43
Verschlüsseln/entschlüsseln 7
Warum verschlüsseln? 3

—U—

Überschreiben und Löschen der Originaldateien nach Ver-/Entschlüsselung 34
Unterschied zwischen der Verwendung eines Aliasnamens und Schlüssels zur Verschlüsselung 18

Copyright © 2000 Norman

—V—

Ver-/Entschlüsselung, Statusmeldung 37
Verarbeiten der Originaldateien 34
Vergessenes Privacy-Anmeldekennwort 75
Verknüpfung zum Privacy-Dialogfeld 12
Verlieren der Textformatierung nach der Verschlüsselung 43
Verschlüsseln
  Dateien, selbstentschlüsselnd 47
  Dateien, Standard 45
  Datenträger, selbstentschlüsselnd 55
  Datenträger, Standard 52
  E-Mail, vollständig, mit oder ohne Anhänge 41
  Grafiken/Bilder 45, 48, 51
  Inhalt der Zwischenablage 43
  Rekursive Verzeichnisse 49, 54
  Systembereiche eines Datenträgers 5
  Text 43
  Verzeichnisse, selbstentschlüsselnd 51, 63
  Verzeichnisse, Standard 48
  Wo 6
Verschlüsseln & Entschlüsseln von Dateien 7
Verschlüsselter Text, Erscheinungsbild 44
Verschlüsseltes Verzeichnis, Verschlüsseln eines Teils oder des gesamten 7
Verschlüsselung
  Anzeigen einer Statusmeldung nach 37
  Datenträger, Elemente, die nicht verschlüsselt werden können 52, 55
  Info 4
  Max. Textmenge, die verschlüsselt werden kann 43
  Modul 9
  Rekursiv 6
  Unterschied zwischen der Eingabe eines Schlüssels und der Auswahl eines Aliasnamens 18
  Warum? 3
  Was Sie verschlüsseln können 4
  Ziehen und Ablegen 46, 49, 63
Verwenden des Dialogfelds Schlüsselwahl 40, 57
Verzeichnisse
  Ablaufdatum, festlegen 50
  Entschlüsseln 6
  Entschlüsseln eines Teils oder des gesamten 7
  Komprimieren vor der Verschlüsselung 50
  Komprimierung 4
  Rekursive Verschlüsselung 49, 54
  Selbstentschlüsselnd 8
  Sicher löschen der Originale nach Ver-/Entschlüsselung 34
  Verschlüsseln 6
  Verschlüsseln, selbstentschlüsselnd 51
  Verschlüsseln, Standard 48
  Zwei Möglichkeiten zum Verschlüsseln 6
Verzeichnisse entschlüsseln, selbstentschlüsselnd 63
Voreinstellungen in Privacy
  Einstellen 37
  Schlüssel bestätigen 36
  Statusmeldung nach der Ver-/Entschlüsselung 37
Vorgehensweise nach dem Anmelden 14

—W—

Wechseldatenträger
  siehe Datenträger
Weiche Schlüssel 18
Wiederherstellen von Dateien von der

Copyright © 2000 Norman

Festplatte 34
Windows Explorer, Rolle beim Verschlüsseln/Entschlüsseln 6

—Z—

Zeitstempel, beibehalten nach Verschlüsselung/Entschlüsselung 34
Ziehen und Ablegen
Dateiverschlüsselung 46, 63
Verzeichnisentschlüsselung 69
Verzeichnisverschlüsselung 49
Zugriff-Zeitstempel 34
Zusammengehörige Aliasnamen in Privacy 19
Zusätzliche Sicherheitseinstellungen 36
Zwischenablage
Entschlüsseln des Inhalts 60
Verschlüsseln 7
Verschlüsseln des Inhalts 43

Copyright © 2000 Norman